Bring Your Own Device (BYOD) Policy

As mobile devices become ubiquitous, it is becoming common for employees to bring personal devices, such as laptops, phones, and tablets, to their workplaces and connect them to the employer's network. Employees may also utilize these devices for work purposes, such as accessing work emails and documents, texting or calling about work-related matters, etc. In addition to using personal devices at the workplace, employees may desire using them to get work done when away from the usual work location under various circumstances, e.g., telecommuting from home, working from a coffee shop, traveling for personal or business purposes, etc. The increasing practice of using personal devices for work purposes is commonly referred to as Bring Your Own Device (BYOD).

While BYOD often provides an individual with increased flexibility and convenience, it may violate important aspects of the employer's security and privacy policies. A famous example is the security violations that resulted from the choice by Hillary Clinton to use a private email server out of convenience. To mitigate and manage the risk posed by BYOD practices and to strike a reasonable balance between personal convenience for employees and security and privacy protections for organizational assets, companies are beginning to specify an explicit policy pertaining to BYOD.

Imagine that you are responsible for setting security and privacy policies for a company that handles billing and other financial matters pertaining to patients at various healthcare facilities throughout the US. As such, the company's clients include healthcare facilities as well as insurance providers. Since the company handles patient data, it must abide by applicable provisions of HIPAA (Health Information Portability and Accountability Act). The company has several offices spread across a number of US states and employs more than 20,000 full-time individuals in various roles, ranging from administrative assistants who manage office tasks to software developers who build and manage software for the systems used by the company. Additionally, the company has nearly 2,000 sales persons who are typically visiting current or prospective clients and working on-the-go. Non-sales employees may also choose to telecommute as needed, often during the evenings and weekends, but sometimes also during the week.

Your task is to write a BYOD policy for the company. The policy must specify goals and objectives along with requirements and guidelines designed to meet those objectives. The requirements and guidelines may include permissible as well as forbidden practices, and it may provide example use cases. Take into account various trade-offs between security and privacy considerations of the company and convenience, flexibility, and productivity desires of the employees. A good policy will succinctly capture the diversity and nuance of work practices and incentives. At the same time, it must not violate laws and regulations (e.g., HIPAA). The policy should provide information on enforcement as well as consequences for violations. An effective policy will be sufficiently specific to facilitate comprehension and implementation and sufficiently general to be broadly applicable.

Your mid-term paper will be composed of the following three components:

1. A BYOD policy for the company that covers relevant security and privacy aspects. The policy should cover use of personal devices at work locations as well as off-site. It should be similar in tone and style to the privacy and security policies we have read and discussed in class.
2. A justification of your policy specification. Describe the various trade-offs and other considerations you took into account and provide the rationale behind the choices you made in specifying the policy. You may use and cite external sources beyond what we have covered in class, but you are not required to do so. Do not cite Wikipedia articles.
3. A discussion of how the policy and your justification connect to the various course readings and presentations, discussions, videos, and activities in class. Include appropriate citations when referring to the readings.

Your overall score for the paper will be allocated as: BYOD policy (50%), Justification (25%), and Connection to Course Materials (25%). There is no single right answer. Your score for the policy will depend on the effectiveness of the tradeoffs made by the policy to achieve optimal levels of operational security and privacy that fits the organizational context of the company. The scores for the other two components will be determined by how well you justify and explain the choices made in the policy and how accurately you connect your rationale to course materials.

It is expected that thoughtful consideration of each component will require about two single-space pages per component. However, the score will be based on the quality of the paper, independent of length.

Due: ***Thursday, March 9th by 11:59 pm.***