**CS4411 Assignment 4**

Micah Hanmin Wang

#3631308

Q1. I’m writing in ISO standards.

A Random IT Co.’s Acceptable Use Policy be like:

1. Acceptable Use

Users should be aware that all use of Random IT Co.is subject to monitoring as described in this Policy and as such, Users have no right to, or exception of, privacy with respect to their use of Random IT Co., subject to applicable laws and terms of use. Incidental and occasional personal use of Random IT Co. is permissible as long as it does not interfere with workplace productivity or the Company's systems or business operations, does not pre-empt any business activity, does not consume more than a trivial amount of the Company's resources and is lawful.

2. Unacceptable Use

- Download any malicious programs or software to their working laptops

- Download games or any entertainment software on their working laptops

- Lend, sell, donate their working laptops.

- Engage in activities for personal gain or use any company’s assets for commercial use or business purposes, without Company’s permission.

- Access, use or disclose confidential information without Company’s authority.

- Viewing any inappropriate content online

- Leaking your password and any sensitive information to your other people, including your families.

- Sending confidential company information without prior authorization from your manager.

- Send any unsolicited or malicious emails to other people using working email account.

- Click any phishing emails using working email account.

- Violate any applicable laws.

- Install or use peer-to-peer file-sharing programs or access those types of networks.

- Use Company’s resources in a manner where violates applicable laws.

Discussion:

My company’s corporation is a lot broader in terms of their scope of writing. They use something like:

‘All employees, agents, suppliers, and contractors are responsible for the proper use of Company assets. This responsibility applies to all the Company's assets, including your time, work, and work product; cash and accounts; physical assets such as inventory, equipment, vehicles, computers, systems, facilities and supplies; intellectual property, such as patents, copyrights, trademarks, inventions, technology and trade secrets; and other proprietary or non-public information.’

And ‘You must take reasonable steps to ensure that the Company receives good value for Company funds spent.’

…which uses more formal and general definition when talking about what’s allowed to do and what’s not allowed to do.

Additionally, they emphasized on protecting company’s information rather than regulating personal use of company’s IT assets. Also focus on more business aspects.

However, they don’t seem to include any specific details, like the use of working laptop and passwords policy I mentioned above.

Their policy is stricter, even though not much details include, but it covered almost everything needed.

They apparently need to include more details, procedures when talking about the Acceptable User Policies.

Q2. A Business Continuity Plan (BCP) is a prevention and recovery systems for potential threats, such as natural disasters or, more commonly, cyber-attacks. It is designed to protect personnel and assets and make sure they can function quickly when disaster strikes. BCPs should be tested to ensure there are little-to-no weaknesses in your systems, which can be identified and corrected. BCPs should include determining how the risks will affect operations, implementing safeguards and procedures to mitigate the risks, do testing regularly to ensure the BCP is working, and always make the relative components of BCP up to date. BCP is an important part of business. If a loss happens, the threat and cost mean a loss of tremendous amount of revenue and even higher costs, which leads to a drop in profit. The Rogers incident happened on early July 2022 is an excellent example of this. BCP is generally conceived in advance and involves input from key stakeholders and personnel.

Business Impact Analysis (BIA) helps identify areas that need attention during any type of business change or event. When you use BIA to understand the areas and severity of an impact, it gives you a roughly roadmap to formulate strategies to minimize the disruption or loss. BIA is a method to reduce risks, guide changes, and improve Business Continuity Plan (BCP). The need for understanding BIA applies every single person in the company/organization.

Disaster Recovery Plan (DRP) is a plan for when an incident happens to the company, the company should have a fast-recovery or a back-up plan to go forward with, ensuring their availabilities and preventing from mass loss. Every business should develop IT Disaster Recovery Plan. It should cover hardware (servers, desktops, laptops, wireless devices), software applications and most importantly – data. The plan should include a strategy to ensure that all critical information is backed up. The National Institute of Standards and Technology (NIST) has several computer security division special publications that can be referred to for any corporation’s DRP.