

Programme Name: \_\_\_\_\_\_\_\_**BCS HONS**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Course Code: \_\_**CSC 2734**\_\_\_\_\_\_\_

Course Name: \_\_\_\_\_\_\_\_**Information System Security**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Assignment 2**

Date of Submission: \_\_\_\_\_\_**5/16/2021**\_\_\_\_\_\_\_\_\_\_\_\_\_

**Submitted By: Submitted To:**

Student Name**: Dipesh Tha Shrestha** Faculty Name**: Manoj Gautam**

IUKL ID: **041902900028** Department**: LMS**

Semester**: Third Semester**

Intake**: September 2019**

1. **Explain the role of information security in employee termination.**

**Answer:** As we know, Employee termination refers to the end of an employee’s work with a company. An employee may be terminated from a job of their own free will or following a decision made by the employer. Some cause of employee termination are Low performance, Violation of Company Rules, Employee Disciplinary Action, Harassment of any sort, be it sexual, physical, mental, or emotional, Lack of cooperation and progressive discipline or Leaking information to competition etc. The employee termination process should focus on severing all ties between the employee and the company. This includes blocking the employee's internal access to all company data. Information Security should immediately revoke the former employee's computer, network, and data access. Remote access should also be removed, and the former employee should be dispossessed of all company-owned property, including technological resources such a notebook computer and intellectual property such as corporate files containing customer, sales, and marketing information. Just as the granting of access and security clearances should be documented for future reference, the revocation of access should also be documented, especially for legal purposes. The goal, of course, should always be to revoke access in ways that make good business sense financially, technologically, and legally. **The role of information security in employee termination are given below:**

* **Change any shared account passwords that were known by the employee**

While typically discouraged, it is often a requirement that multiple users share the password to a single account.  For example, the password to a local Administrator account or an application’s super-user account may be shared by more than one employee.  If the employee is in possession of one of these shared passwords, it should be immediately changed.

* **Retrieve computing hardware from the employee**

Upon separation, all computing hardware issued to an employee will need to be collected.  This includes but is not limited to any University-issued laptops, desktops, computing peripherals, cell phones and hardware tokens.  Any hardware token the employee may have should be immediately returned to the appropriate administrator.  All other hardware can be re-used as deemed appropriate by the manager of the employee. In those limited circumstances where ownership of computer equipment is transferred to the separating employee, the following steps should be considered:

* Archive any business related documents, as directed by the separating employee’s management
* Remove all non-public information that is owned or licensed by the University
* **Change and disable application-level passwords and accounts.**

 Start with the business-critical applications first, such as CRMs and Financial applications. Don't forget other commonly overlooked applications such as Dropbox, which can be configured to sync data to a personal home machine.

* **Preemptive Preservation of Data**

Every company needs to have data redundancy and retention policies that satisfy its business needs and adhere to applicable laws. Such policies address the backup, restoration, and preservation of corporate data in general. However, a company should also enact policies that detail when and how IT should go about preserving potentially and particularly sensitive data, records, logs, and other material that could be of legal significance, should the company and former employee wage a legal battle. This is especially important in the case of a former employee who held a high-level position or left the company under a cloud of suspicion.

* **Change the employee's password and disable their Active Directory (AD) and/or 365 user account(s).**

This may seem redundant, but in the heat of employee termination, taking these two steps together greatly increases the chances that at least one of them gets done if the other one is missed. Remove the employee from all access to AD and/or 365 groups and memberships, as well as phone systems account, social media accounts, etc. This helps ensure any group-based permissions are removed and minimize future reminders to other employees about the termination. Disable their computer account. This is an additional step that helps reduce any chance of re-entry into your systems.

1. **Explain contingency planning with its components.**

**Answer**: Contingency planning aims to prepare an organization to respond well to an emergency and its potential humanitarian impact. Developing a contingency plan involves making decisions in advance about the management of human and financial resources, coordination and communications procedures, and being aware of a range of technical and logistical responses. Such planning is a management tool, involving all sectors, which can help ensure timely and effective provision of humanitarian aid to those most in need when a disaster occurs. Time spent in contingency planning equals time saved when a disaster occurs. Effective contingency planning should lead to timely and effective disaster-relief operations A contingency plan acknowledges that disaster can happen: the organization must design a plan to accommodate the survival of organizational operations in the event of a flood, fire, earthquake, electrical disturbance, or other unexpected events that can disrupt the organization’s systems. Risk analysis should offer guidance on the likelihood of various contingencies, and in what resources to invest providing such recovery methods as off-site systems, backups, and so on. Several references discuss contingency planning.

**There are five common components that contingency plans should have:**

**Information:**

At the heart of a contingency plan is the ability to identify when a contingency exists. For some companies (including those who have made the jump to Stage 2), the information is a metric or set of metrics. For others (including those who are still operating as Stage 1 businesses), it is a more instinctive feeling about the business.

**Boundary conditions:**

Once a company has the set of information it is going to use to assess the situation, it then must decide under what conditions it will say a “contingency that must be addressed” exists. In other words, what is the “comfort zone” for the metrics, and where are the edges of that zone.

**Levers:**

A contingency plan should also consider what the levers are that the business can use to correct its path. These levers might be cutting administrative spending, increasing sales visits, deferring salary increases, or changing an approval process. Levers should focus either on revenue impact or cost impact. Because it’s unlikely that any one lever will be able to impact both areas, and because the business might face situations that need to manage revenue or cost, it is best to develop a portfolio of levers that you can work with.

**Decision process:**

With information, boundaries, and levers in place, the business should think through how it will actually decide to use the levers if the information indicates that a boundary has been crossed. This will vary from company to company. Some will have a preset decision-making process, so that the rules are clear before the company gets into a contingency. Others are comfortable leaving it loose until they are faced with the situation.

**Scenarios:**

A contingency plan with the four components described above is enough to manage contingencies effectively. To take the preparation up another notch – and enable a management team to feel confident that it is prepared – the team can also create 2-5 higher-probability scenarios, to think through what each of the elements would look like in each scenario, and what potential issues could be. Scenarios could be “We win three big projects at the same time” or “We lose our biggest customer” or “Our bank cancels our line of credit.”

1. **Asset valuation is the process of assigning financial value or worth to each information asset. Explain FIVE (5) components that include assets valuation**

**Answer:**

Asset valuation is the process of determining the fair market or present value of assets, using book values, absolute valuation models like discounted cash flow analysis, option pricing models or comparable. Asset valuation simply pertains to the process to determine the value of a specific property, including stocks, options, bonds, buildings, machinery, or land, that is conducted usually when a company or asset is to be sold, insured, or taken over. The assets may be categorized into tangible and intangible assets. Valuations can be done on either an asset or a liability, such as bonds issued by a company.

**FIVE (5) components that include assets valuation are:**

* Intellectual property value

The value of a new product or service provided to a customer is frequently unknown. For example, what is the value of a cancer cure, a logo design, or a slogan, and so on. Because intellectual property is intangible and according to the exhumations of the human mind, it is related but separated from how much or the cost of new intellectual properties.

* Value sharing the information

Information is a necessary component for starting anything, and before even beginning to use a product or security, all users require detailed information for the developers and makers, as well as some for the users who will use it. As a result, information should be provided to users who require it at a low cost. The cost or provision of information is determined by the value and importance of the information.

* Value retained from past maintenance of the information asset

The main place where money is spent when an app is bought or developed, data, security, and so on, is on asset maintenance. Over the useful life of data or software, the majority of money is spent on maintenance. The cost of maintenance can be estimated based on the asset's updates, modifications, services, and systems that have been developed or updated. Because maintenance should be performed as frequently as possible or as needed to provide users with easy access to the asset, introduce something new, and upgrade the security and system.

* Loss of productivity while the information assets are unavailable

It will take time to recover lost information after it has been lost, as it may be critical. In this case, the cost must be estimated using the previous cost as well as some new ones. Because it costs money to recover data that has been lost due to hackers or not being backed up. However, following the attacks, there was a loss of security and new alternatives. Employee hours, alternative costs, new security, and a lack of productivity will all be a hindrance to the operation's progress.

* Value derived from the cost of protecting information

The cost of protecting information is determined by the value of the information. And the cost of protection is determined by which part of the information is most valuable and how valuable the information is. The amount of money spent on protecting information is determined by the value of the information, creating an endless cycle of protection. The amount of money spent on protecting information is determined by the value of information, creating an endless cycle of protection that begins with the value of information.

**Thank you**