# CYB 200 Module Two Case Study Template

After reviewing the scenario in the Module Two Case Study Activity Guidelines and Rubric document, fill in the table below by completing the following steps for each control recommendation:

1. Specify which Fundamental Security Design Principle best applies by marking all appropriate cells with an *X*.
2. Indicate which security objective (confidentiality, availability, or integrity) best reflects your selected control recommendation.
3. Explain your choices in one to two sentences, providing a selection-specific justification to support your decision.

| **Control Recommendations** | **Least Privilege** | **Layering (Defense in Depth)** | **Fail-Safe Defaults / Fail Secure** | **Modularity** | **Usability** | **Security Objective Alignment (CIA)** | **Explain your Choices (1-2 sentences)** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Automatically lock workstation sessions after a standard period of inactivity. (Completed as an example) |  | X |  |  |  | C | I chose layering because it adds another layer of protection for the confidentiality of our data. |
| If possible, close and lock your office door when leaving your computer. |  |  | X |  |  | C | Fail-Safe Defaults / Fail Secure because if a user is not giving the access to the room, the user will not have access to the computer, and the confidentiality of the information will remain intact. |
| Use technology to make sure that only authorized software executes, and unauthorized software is blocked from executing on assets. | X | X |  |  |  | A | Least Privilege and Layering. Least Privilege ensure that the user has minimal access to perform duties which block them to perform risky duties and layering because involve of check to access the data or services. |
| Use automated tools to inventory all administrative accounts to ensure that only authorized individuals have elevated privileges. | X |  | X |  |  | C | Only authorized individuals can have access to elevated privilege, if users don’t have access, it will deny entry. Which would ensure that the data will no be accessed. |
| Use system configuration management tools to automatically reapply configuration settings to systems at regularly scheduled intervals. |  |  |  | X |  | A | Modularity is my choice since a big task is breaking down into small task and make it available for the users. |
| Maintain an inventory of all sensitive information stored or transmitted by the organization's technology systems, including those located on site or at a remote location. |  | X |  |  |  | C | Implementing different levels of security and distributed in different storage will preserve the confidentiality of the information. |
| Use approved whole-disk encryption software to encrypt the hard drive of all mobile devices. |  | X |  |  |  | C | The encrypted software would encrypt hard drives from all the phones which describe the way that hard drives have layers of security to keep confidentiality of the hard drives. |
| If USB storage devices are required, software should be used that can configure systems to allow the use of specific devices. |  |  |  | X |  | A | The software is secure so it will maintain the security in the specific devices which would be available to the users. |
| Configure systems not to write data to external removable media, if there is no business need for supporting such devices. | X |  |  |  |  | I | The integrity of the data and user will be protected by not allowing external non-authorized users write into the data. |
| If USB storage devices are required, all data stored on such devices must be encrypted. |  |  |  |  | X | C | Encryption in the devices would help to prevent any access to non-authorized users and the usability will let the user share their information even if they do not have the knowledge of how the information is stored. |
| Protect all information stored on systems through the use of access control lists. These access control lists enforce the principle that only authorized individuals should have access to the information based on approved business need. | X |  | X |  |  | C | The users must be authorized to get access to the information stored which would be preserved confidential for non-unauthorized users. |
| Require multifactor authentication for all user accounts, on all systems, whether managed on site or by a third-party provider. |  | X |  | X |  | C | Authorized users are required to have authentication identification and keep the information and data of confidential. |

After you have completed the table above, respond to the following short questions:

1. How might you work with someone like Dr. Beard to cultivate a security mind-set that is more in line with the organization’s ethical norms? Hint: Consider his attitude, his past behaviors, and his opinion about organizational policies.
   1. Dr. Beard’s scenario provides us with a huge representation of how malicious users are available to get into private information because of human errors. First, Dr. Beard is aware of the hospital policies which specify that accessing patient files outside the location is prohibited. Dr. Beard’s excuse is that he is unable to finish his work, but he’s not willing to stay in the hospital to work on it, instead taking it outside. Second, the hard drive was abandoned in a car unattended even knowing that contained important information. Finally, Dr. Beard has the username, and the password written down with easy access for any person to access the computer.
2. How would you help the hospital better secure its patient files? Make sure to incorporate at least one data state (data-at-rest, data-in-use, or data-in-motion) and one of the control recommendations from your completed table in your response.
   1. One of the most important things to secure patients’ files is by educating employees on every aspect, so it will be a little more complicated to have access to files through employees. Encryption files would be beneficial for any non-secure access and denied access to patient files remotely. Implementing the use of VPN when the data-in-use and restricting access by giving privileges to authorized users. Multiple authentication factors ensure that only authorized users have access to it.