Free system analysis: centralized university network data storage research paper ...

Business, Management

\n[toc title="Table of Contents"]\n

\n \t

\n[/toc]\n \n

System Background

The capacity of a university system to hold as much information as needed plays a great role on how modern data management is handled in organizations and institutions that cater to a huge number of population of individuals needing to be served and given attention to. Having a centralized data system that stores the major information about the general population being served allows the administrators to see to it that every operation and every institutional procedure is given direct attention to.

Notably, the centralized data network used by the Istanbul Technical University follows the same pattern of function. However, being that the institution utilizes the said system for a relatively high number of individual information placed within the system, there are some issues that need to be given attention to especially in terms of data safety and controlled access on the part of the individuals and officers who are supposedly able to control the data encoded into the data-network and other information separated from one section to another thus making access points exclusive for administrators [while some other information are made available for public access].

Issues and Flaws of the System

As noted from the first project delivery, while the system used by ITU is effective enough in completely containing all data in a single data storage network, it could be observed that there are some specific flaws that could be identified to have distinct impact on how the whole system works and how effective the system is in determining the information management that the institution needs to embrace. Practically, these issues are related to security and access points. Some of the said problems could be identified herein as follows:

- Security of Information

The data encoded into the system does provide a system of developed operation on how administrators and the students themselves access information that they need whenever necessary. Practically, these system allows encoders and data-users to gain efficient access and control of the information stored into the network. However, the security measures taken into account to protect personal or confidential information is quite weak especially when it comes to making an assumptive control on how data-protection is given particular attention to.

- Separation and Categorization of Data

One of the ways by which data is exclusively protected for those who are allowed to see through the system is through categorizing the information according to the value that they represent for particular users of the system. Notably, it could be understood that there are some set of data that should only be available for administrators, while some others could be used by the students and the public trying to see through the different operations and

other information about the institution [according to their point of interest]. Given that the network is easily accessible to everyone connected to the net, malicious operations and manipulation of data is expected to occur.

- Firewalling Data Categories

Through categorizing the data within the network, the institution is able to make sure that every information contained in it is properly protected. Expectedly, this requirement intends to directly establish a sense of control on how modern systems of data control could be realized accordingly especially in terms of establishing technical firewalls that are designed to give attention to how each data is treated by each user of the website. The visitors coming into the website with a much less controlled connection to the organization or the institution should be given limited access to the information shared by the organization for the public to appreciate and use.

- Authorization of Access Points

These pass keys would indicate the overall control and allowable actions that the users have on the stored data. Understandably, the system itself will recognize the pass keys through code-categorization. With such identification points, the users are given proper access to the specific data they need to manage and read through.

These problems often imply a sense of distinction on how data within the system network is protected and controlled according to the level of authority that users have in relation to the operations of the institution. For instance, administrators ought to have a separate access point and pass key apart from students aiming to have connection with the institution’s network. Relatively, this process of establishing keys of identification intend to

mandate the conditions by which users are to be given the chance to access necessary data they need to give attention to.

Loop Diagram

Suggested Solutions

Firewalling: Information firewalling is assumed to have a great impact on how information stored within the network is defined and categorized according to their value of importance to the institution. Firewalling involves the utilization of codes that are dedicated towards making an access point that is fully manageable by authorized individuals only. Firewalling involves the need to

Conclusion