Week 2 Assignment

[Name of the Writer]

[Name of the Institution]

Week 2 Assignment

The data classified in the context of commercial organizations are: confidential, proprietary, sensitive but maybe public as well. Every company has the data that is very sensitive that contains all the information regarding company assets and polices. If this data is leaked then it causes serious damage to the company. On the other hand, confidential data is less restrictive than sensitive data, however if leaked, the company can face serious consequences. Private data include cell numbers, addresses, etc. If this data is disclosed, it cannot cause a threat to the company although this may cause distress to the employees. The data that is released on a limited basis is called as proprietary data. For instance, Samsung brand cell phone specifications are considered proprietary until the release of the phone in the market. Public data is available for the people such as the company’s details regarding the list of services it provides.

The military data is classified as confidential, secret and top secret. Confidential data include the information which, if disclosed can cause severe threat to the national security. For instance, the information of a number of officials deployed in any area or the design of the weapon is considered confidential. The secret data contains the information which if disclosed can cause more severe damage to the national security such as information regarding future military plans. The top-secret data is the data which if disclosed can cause exceptionally severe damage to the entire national security such information regarding war plan and intelligence agency plans etc. (Rushby, 1984).

The responsibility of a team in different roles are as follows:

**Data Owners**

In any company, it is the role of senior management to protect the specific data of the company while also setting a data security plan. Only after their approval, the data can be accessed. They also deal with any violations and threats to the data.

**Data Custodian**

The maintenance and protection of data is the responsibility of the data custodian. Mostly, the members of the IT department are the data custodian. Their duties include to add or remove data access, backup, validation and restoring the data while also recording the daily activity.

**System Owner**

The owner of the system can be responsible for one or more systems that may contain the data of different owners. The key responsibility of the system owner is to integrate security into applications while also make decisions regarding system purchasing. They have to ensure that the system is accessed properly and report vulnerabilities of the system.

**Administrator**

The key responsibility of a security administrator is to manage new systems while implementing security software, issuing passwords and testing the system’s security as well. Generally, the network administrator is responsible for ensuring the configuration of system and servers hardware while also installing the latest updates and managing the system’s vulnerability.

**Analysts**

Analysts develop policies and guidelines. Their role in an organization is to define different elements of security programs and follow through each step to ensure the proper working (Wright, 2008).

**Users**

Users have limited access so that they can perform their functions. However, being a user it is necessary to comply with the policies and guidelines of the organization.

TCB of a computer system consists of hardware, software, and firmware. All of these are critical to the system’s security thus ensuring organization security. TCB’s primary security mechanisms are a security policy, authentication, identification, and auditing. All the security controls, system location, and software are built-in in the operating system of TCB. It also monitors functions like input and output operation of the system while protecting memory, process activation, and execution of domain switching (Peltier, 2016). TCB hardware includes physical works station such as dell computers and CPU. TCB software includes the system’s operating system while TCB firmware includes the updates regarding the identified system’s vulnerability or increase security.

**References**

Rushby, J. (1984, September). A trusted computing base for embedded systems. In *Proceedings 7th DoD/NBS Computer Security Conference* (pp. 294-311). Citeseer.

Wright, C. S. (2008). *The IT regulatory and standards compliance handbook: How to survive information systems audit and assessments*. Elsevier.

Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. Auerbach Publications.