Principles of Cybersecurity Reference Guide

Cybersecurity principles of IT focus on a set of practices intended to keep a corporate infrastructure secure. These practices include, but are not limited to, system, data, internal, external, and physical security. The principles are designed to prevent unauthorized access or alterations of a corporate environment. By understanding how cybersecurity principles are defined, they can then be used to develop a comprehensive, corporate-specific security policy.

In a Microsoft Word document, create a table that defines the principles of cybersecurity listed below. Hint: use landscape orientation to better format your table.

* Separation (of domains/duties)
* Isolation
* Encapsulation
* Modularity
* Simplicity of Design (Economy of Mechanism)
* Minimization of implementation (Least Common Mechanism)
* Open Design
* Complete Mediation
* Layering (Defense in Depth)
* Least Privilege
* Fail-Safe Defaults (Open/Secure)
* Least Astonishment (Psychological Acceptability)
* Minimize Trust Surface (Reluctance to Trust)
* Usability
* Trust Relationships

For each of the principles listed, include the following:

* Definition of the cybersecurity principle (1–2 sentences written in your own words).
* Description regarding why each principle is important to security and how it enables the development of security mechanisms to implement desired security policies.
* Include an in-text citation for each principle listed.

While APA style is not required for the body of this assignment, solid academic writing is expected, and documentation of sources should be presented using APA formatting guidelines, which can be found in the APA Style Guide, located in the Student Success Center.