**Information System Engineering Principles Policy**

1. Principle of Security Integration
   * Security should be an integral part of the overall system design.
   * Security measures should be fully integrated into the system life-cycle.
   * Security policies, requirements, and evaluations should be considered during system engineering, design, implementation, and disposal.
2. Principle of Secure Software Development
   * Developers should receive adequate training in secure software development.
   * Secure coding practices and standards should be followed during system development.
   * Configuration control, integration, and testing of secure software should be emphasized.
3. Principle of External System Insecurity
   * External systems should be assumed to be insecure until proven otherwise.
   * System security features should be designed considering the differences in security measures between internal and external systems.
4. Principle of Information Protection
   * Data should be protected while being processed, in transit, and in storage.
   * Security measures should preserve data integrity, confidentiality, and availability during various stages of information handling.
5. Principle of Open Standards
   * Security measures should be based on open standards for portability and interoperability.
   * Hardware and software solutions should incorporate interoperability and portability to enhance security capabilities.
6. Principle of Layered Security
   * Multiple layers of security should be implemented to address specific threats.
   * Layered security reduces the risk of a single point of vulnerability and enhances overall system protection.
7. Principle of Isolation
   * Public access systems should be physically or logically isolated from critical resources.
   * Network architecture designs, such as demilitarized zones and screened subnets, should be used to establish security layers.
8. Principle of Least Privilege
   * Access privileges should be limited to the minimum necessary for required functions.
   * Role-based access controls should be implemented to assign permissions based on user roles.
   * Separation of duties should be maintained to ensure proper security controls.
9. Principle of Secure System Disposal
   * Proper procedures should be followed for the secure disposal of system assets.
   * Information should be purged from system hard drives, memory, and other media to prevent unauthorized retrieval.

Adherence to these principles ensures that information systems are designed, developed, and operated with security as a fundamental consideration. All personnel involved in system engineering and development should comply with this policy to maintain a secure information environment.