1. Purpose
<Organization Name> <Insert Organization Mission Here>. This policy establishes the Enterprise Security Planning Policy, for managing risks from inadequate security planning through the establishment of an effective security planning program. The security planning program helps <Organization Name> implement security best practices with regard to enterprise security planning, preparation, and strategy.

2. Scope
The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by <Organization Name>. Any information, not specifically identified as the property of other parties, that is transmitted or stored on <Organization Name> IT resources (including e-mail, messages and files) is the property of <Organization Name>. All users (<Organization Name> employees, contractors, vendors or others) of IT resources are responsible for adhering to this policy.

3. Intent
The <Organization Name> Information Security policy serves to be consistent with best practices associated with organizational Information Security management. It is the intention of this policy to establish a security planning capability throughout <Organization Name> and its business units to help the organization implement security best practices with regard to enterprise security planning, preparation, and strategy.

4. Policy
<Organization Name> has chosen to adopt the Security Planning principles established in NIST SP 800-53 “Security Planning,” Control Family guidelines, as the official policy for this domain. The following subsections outline the Security Planning standards that constitute <Organization Name> policy. Each <Organization Name> Business System is then bound to this policy, and must develop or adhere to a program plan which demonstrates compliance with the policy related standards documented.

- **PL-1 Security Planning Policy and Procedures:** All <Organization Name> Business Systems must develop, adopt or adhere to a formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
- **PL-2 System Security Plan:** All <Organization Name> Business Systems must develop a security plan for the company information assets that:
  - Is consistent with the organization’s enterprise architecture.
  - Explicitly defines the authorization boundary for the system.
- Describes the operational context of the information asset in terms of missions and business processes.
- Provides the security category and impact level of the information asset including supporting rationale.
- Describes the operational environment for the information asset.
- Describes relationships with or connections to other information systems.
- Provides an overview of the security requirements for the system.
- Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions.
- Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.
- PL-3 Rules of Behavior: All <Organization Name> Business Systems must establish and make readily available to all information asset users, the rules that describe their responsibilities and expected behavior with regard to information and information asset usage. In addition, they must receive signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information asset.
- PL-4 Privacy Impact Assessment: All <Organization Name> Business Systems must conduct a privacy impact assessment of the information assets in accordance with Information Security Risk Categorization policy.
- PL-5 Security-Related Activity Planning: All <Organization Name> Business Systems must plan and coordinate security-related activities affecting company information assets before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.
Appendix A – References

The following references illustrate public laws which have been issued on the subject of information security and should be used to demonstrate <Organization Name> responsibilities associated with protection of its information assets.

