1. Purpose
<Organization Name> <Insert Organization Mission Here>. This policy establishes the Enterprise Personnel Security Policy, for managing risks from personnel screening, termination, management and third-party access, through the establishment of an effective security planning program. The personnel security program helps <Organization Name> implement security best practices with regard to personnel screening, termination, transfer and management.

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 personnel security capability throughout <Organization Name> and its business units to help the organization implement security best practices with regard to personnel screening, termination, transfer and management.

4. Policy
<Organization Name> has chosen to adopt the Personnel Security principles established in NIST SP 800-53 “Personnel Security,” Control Family guidelines, as the official policy for this domain. The following subsections outline the Personnel Security 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 the standards documented.

- PS-1 Personnel Security Procedures: All <Organization Name> Business Systems must develop, adopt or adhere to a formal, documented personnel security procedure that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
- PS-2 Position Categorization: All <Organization Name> Business Systems must:
  - Assign a risk designation to all positions.
  - Establish screening criteria for individuals filling those positions.
  - Review and revise position risk designations on a tri-annual basis.
• PS-3 Personnel Screening: All <Organization Name> Business Systems must screen individuals prior to authorization access to the information asset. In addition, <Organization Name> Business Systems must rescreen individuals every seven years.

• PS-4 Personnel Termination: All <Organization Name> Business Systems must upon personnel termination:
  o Terminate information asset access.
  o Conduct exit interviews.
  o Retrieve all security-related organizational information system-related property.
  o Retain access to organizational information and information assets formerly controlled by terminate personnel.

• PS-5 Personnel Transfer: All <Organization Name> Business Systems must review logical and physical access authorizations to information assets/facilities when personnel are reassigned or transferred to other positions within the organization on a quarterly basis.

• PS-6 Access Agreements: All <Organization Name> Business Systems must ensure that individuals requiring access to organizational information and information assets sign appropriate access agreements prior to being granted access. In addition, <Organization Name> Business Systems must review/update the access agreements on a tri-annual basis.

• PS-7 Third-Party Personnel Security: All <Organization Name> Business Systems must:
  o Establish personnel security requirements including security roles and responsibilities for third-party providers.
  o Document personnel security requirements.
  o Monitor provider compliance.

• PS-8 Personnel Sanctions: All <Organization Name> Business Systems must employ a formal sanction process for personnel failing to comply with established information security policies and procedures.
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.


