1. **Purpose**

<Organization Name> <Insert Organization Mission Here>. This policy establishes the Enterprise Audit and Accountability Policy, for managing risks from inadequate event logging and transaction monitoring through the establishment of an effective Audit and Accountability program. The audit and accountability program helps <Organization Name> implement security best practices with regard to event and transaction logging and the retention of audit evidence.

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 an audit and accountability capability throughout <Organization Name> and its business units to help the organization implement security best practices with regard to event and transaction logging and the retention of audit evidence.

4. **Policy**

<Organization Name> has chosen to adopt the Audit and Accountability principles established in NIST SP 800-53 “Audit and Accountability Control Family guidelines,” as the official policy for this domain. The following subsections outline the Audit and Accountability 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.

- **AU-1 Audit and Accountability Procedures**: All <Organization Name> Business Systems must develop, adopt or adhere to a formal, documented audit and accountability procedure that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
- **AU-2 Auditable Events**: All <Organization Name> Business Systems must:
  - Determine that the information asset must be capable of auditing the following events: **User Access and User Transactions**.
Coordinate the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events.

Provide a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.

Determine that the following events are to be audited within the information asset.

- **AU-3 Content of Audit Records:** All <Organization Name> Business Systems produce audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.

- **AU-4 Audit Storage Capacity:** All <Organization Name> Business Systems must allocate audit record storage capacity and configure auditing to reduce the likelihood of such capacity being exceeded.

- **AU-5 Response to Audit Processing Failures:** All <Organization Name> Business Systems must alert designated organizational officials in the event of an audit processing failure. In the event of an audit processing failure, <Organization Name> Business Systems must configure the audit log to (1) stop generating audit records or (2) overwrite the oldest audit records.

- **AU-6 Audit Review, Analysis, and Reporting:** All <Organization Name> Business Systems must review and analyze information asset records periodically for indications of inappropriate or unusual activity, and report findings to designated organizational officials. In addition, <Organization Name> Business Systems must adjust the level of audit review, analysis, and reporting within the information asset when there is a change in risk to organizational operations, organizational assets, individuals, other organizations due to credible intelligence.

- **AU-7 Audit Reduction and Report Generation:** All <Organization Name> Business Systems must provide audit reduction and report generation capability for company information assets.

- **AU-8 Time Stamps:** All <Organization Name> Business Systems must use internal system clocks to generate time stamps for audit records to facilitate logging and monitoring.

- **AU-9 Protection of Audit Information:** All <Organization Name> Business Systems must protect audit information and audit tools from unauthorized access, modification, and deletion.
• AU-10 Non-Repudiation: All <Organization Name> Business Systems must protect against an individual falsely denying having performed a particular action on company information assets. AU-11 Audit Record Retention: All <Organization Name> Business Systems must retain audit records for one year to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

• AU-12 Audit Generation: All <Organization Name> Business Systems must:
  ○ Provide audit record generation capability for the list of auditable events defined in AU-2 for information assets.
  ○ Allow designated organizational personnel to select which auditable events are to be audited by specific components of the system.
  ○ Generate audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.
Appendix A – References

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

