1. Purpose
<Organization Name> <Insert Organization Mission Here>. This policy establishes the Enterprise System and Information Integrity Policy, for managing risks from system flaws/vulnerabilities, malicious code, unauthorized code changes, and inadequate error handling through the establishment of an effective System and Information Integrity program. The system and information integrity program helps <Organization Name> implement security best practices with regard to system configuration, security, and error handling.

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 system and information integrity capability throughout <Organization Name> and its business units to help the organization implement security best practices with regard to system configuration, security, and error handling.

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

- SI-1 System and Information Integrity Procedures: All <Organization Name> Business Systems must develop, adopt or adhere to a formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
- SI-2 Flaw Remediation: All <Organization Name> Business Systems must:
  - Identify, report, and correct information system flaws.
Test software updates related to flaw remediation for effectiveness and potential side effects on organizational information assets before installation.

Incorporate flaw remediation into the organizational configuration management process.

**SI-3 Malicious Code Protection:** All <Organization Name> Business Systems must:

- Employ malicious code protection mechanisms at information asset entry and exit points and at workstations, servers, or mobile computing devices (e.g., email, removable media, and malicious websites) on the network to detect and eradicate malicious code.
- Update malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures.
- Configure malicious code protection mechanisms (e.g., real-time scans, periodic scans, malicious code detection) to protect company information systems and assets.
- Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information asset.

**SI-4 Information System Monitoring:** All <Organization Name> Business Systems must:

- Monitor events on the information asset and detect information asset attacks.
- Identify unauthorized use of the information assets.
- Deploy monitoring devices (1) strategically within the information asset to collect organization-determined essential information, and (2) at ad-hoc locations within the system to track specific types of transactions of interest to the organization.
- Heighten the level of information asset monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.
- Obtain legal opinion with regard to information asset monitoring activities in accordance with applicable federal laws, directives, policies, or regulations.

**SI-5 Security Alerts, Advisories, and Directives:** All <Organization Name> Business Systems must:

- Receive information asset security alerts, advisories, and directives from designated external organizations on an ongoing basis.
- Generate internal security alerts, advisories, and directives as deemed necessary.
- Disseminate security alerts, advisories, and directives to key system owners and stakeholders.
<table>
<thead>
<tr>
<th>&lt;Organization Name&gt;</th>
<th>System and Information Integrity Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department Name</td>
<td>Policy #</td>
</tr>
<tr>
<td>Issue Date:</td>
<td>September 13, 2013</td>
</tr>
</tbody>
</table>

Approved by:

- Implement security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.
- **SI-6 Security Functionality Verification**: All <Organization Name> Business Systems must verify the correct operation of security functions **on an annual basis** and notify the system administrator when anomalies are discovered to ensure timely corrective action.
- **SI-7 Software and Information Integrity**: All <Organization Name> Business Systems must detect unauthorized changes to software within their information asset.
- **SI-8 Spam Protection**: All <Organization Name> Business Systems must employ spam protection mechanisms at information asset entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means. In addition, <Organization Name> Business Systems must update spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.
- **SI-9 Information Input Restrictions**: All <Organization Name> Business Systems must restrict the capability to input information to the information asset to authorized personnel.
- **SI-10 Information Input Validation**: All <Organization Name> Business Systems must check the validity of information inputs for company information assets.
- **SI-11 Error Handling**: All <Organization Name> Business Systems must have company information assets that:
  - Identify potentially security-relevant error conditions.
  - Generate error messages that provide information necessary for corrective actions without revealing company sensitive information in error logs and administrative messages that could be exploited by adversaries.
  - Reveal error messages only to authorized personnel.
- **SI-12 Information Output Handling and Retention**: All <Organization Name> Business Systems must handle and retain both information within and output from the information system in accordance with applicable federal laws, directives, policies, regulations, standards, and operational requirements.
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.


