[Company Name Or Logo]	
Title: Evaluation of Security Policies	**P&P #:**
Approval Date:	**Review:**
Effective Date:	**Security Team**

Purpose:
To ensure that all Security Policies are up to date and effective in ensuring the confidentiality, integrity and availability of sensitive and regulated data created, received, maintained, and transmitted by [Insert Local Gov/K-12 Name]. Periodic policy evaluations are necessary to ensure continued legal compliance and the highest standards for the protection of data.

Scope: This policy applies to organizational information applications, systems, networks and any computing devices, regardless of departmental ownership (e.g., owned, leased, contracted, and/or stand-alone.)

Procedure:

1. Initial Evaluation
    a. Security Policies or Procedures will be initially evaluated against existing regulations to ensure compliance.
    b. Once compliance with the Security Regulations is established, information security policies and procedures will be evaluated on a periodic basis (Insert chosen periodic basis- annually is recommended) to assure continued viability with technological, environmental, or operational changes that could affect the security of sensitive and regulated data. These evaluations will incorporate information security best practices.
2. Periodic Evaluation by Information Security Officer:
    a. The Information Security Officer will review on an on-going basis the viability of [Insert Local Gov/K-12 Name] Security Policies and general approaches taken by departments in their security procedures.
    b. The Information Security Officer will develop and/or recommend any necessary Security Policy or Procedure changes.
3. Periodic Evaluation by [Insert Local Gov/K-12 Name] the Administrative Controls Evaluation Team:
    a. The Evaluation Team will include the Information Security Officer, the Privacy Officer, the Facility Office Manager, the Disaster Recovery Planner, and anyone else the organization deems necessary.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

b. The Evaluation Team will reconvene on an annual basis to evaluate the technical and non-technical viability of [Insert Local Gov/K-12 Name] Security Policies.
c. Any member of the Evaluation Team, the Information Security Officer, or any other person may suggest changes to the Security Policies or Procedures by submitting such suggestions to the Evaluation Team for consideration.
d. The Evaluation Team will review any suggested Security Policy or Procedure change(s) and make a preliminary recommendation.
e. If the Evaluation Team preliminarily recommends a new security standard or a change in security policies or procedures, such new standard or change will be communicated to all departments by the Evaluation Team, who will elicit feedback for a specific period and provide such feedback to the Information Security Officer.
f. The Evaluation Team will consider the feedback received and make a final recommendation on the suggested change to the Information Security Officer.
g. If the Information Security Officer approves the change, such change will be propagated to all departments through policy updates and reminders.
h. The Information Security Officer will update the document, incorporating the updated policies and sign with the appropriate effective date.

4. Evaluation Upon Occurrence of Certain Events
   a. In the event that one or more of the following events occur, the policy evaluation process described in will be immediately triggered:
      i. Changes in the Security Regulations.
      ii. New federal, state, or local laws or regulations affecting the security of sensitive or regulated data.
      iii. Changes in technology, environmental processes or business processes that may affect security policies or procedures.
      iv. A serious security violation, breach, or other security incident occurs.
   b. The Information Security Officer may reconvene the Evaluation Team if deemed necessary based on information received from, but not limited to, the Security Officer or an Internal Audit.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

Violations:
Any individual found to have violated this policy, may be subject to disciplinary action up to and including termination of employment.

Attachments: None

Related Policies: None

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.