**Security Plan**

Owner: Ho Yeung, Lee

Classification: Secret

FIPS-199 SC administrative information = {(confidentiality, HIGH), (integrity, LOW), (availability, LOW)}

Standard: NIST 800-18

Date:

**1.Information System Name/Title**:

* Unique identifier
* name given to the system

**2. Information System Categorization**:

• Identify the appropriate FIPS 199 categorization.

FIPS 199 categorization [Low, moderate, high]:

**3. Information System Owner:**

* Name:
* Title:
* Agency:
* Address:
* email address:
* phone number of person who owns the system:

**4. Authorizing Official:**

• Name, title, agency, address, email address, and phone number of the senior management official designated as the authorizing official.

**5. Other Designated Contacts:**

• List other key personnel, if applicable; include their title, address, email address, and phone number.

**6. Assignment of Security Responsibility:**

• Name, title, address, email address, and phone number of person who is responsible for the security of the system.

**7. Information System Operational Status:**

• Indicate the operational status of the system. If more than one status is selected, list which part of the system is covered under each status.

Operational, Under Development , Major Modification

**8. Information System Type:**

• Indicate if the system is a major application or a general support system. If the system contains minor applications, list them in Section 9. General System Description/Purpose.

**9. General System Description/Purpose**

• Describe the function or purpose of the system and the information processes.

**10. System Environment**

• Provide a general description of the technical system. Include the primary hardware, software, and communications equipment.

**11. System Interconnections/Information Sharing**

• List interconnected systems and system identifiers (if appropriate), provide the system, name, organization, system type (major application or general support system), indicate if there is an ISA/MOU/MOA on file, date of agreement to interconnect, FIPS 199 category, C&A status, and the name of the authorizing official.

**12. Related Laws/Regulations/Policies**

• List any laws or regulations that establish specific requirements for the confidentiality, integrity, or availability of the data in the system.

**13. Minimum Security Controls**

Select the appropriate minimum security control baseline (low-, moderate-, high-impact) from NIST SP 800-53, then provide a thorough description of how all the minimum security controls in the applicable baseline are being implemented or planned to be implemented. The description should contain: 1) the security control title; 2) how the security control is being implemented or planned to be implemented; 3) any scoping guidance that has been applied and what type of consideration; and 4) indicate if the security control is a common control and who is responsible for its implementation.

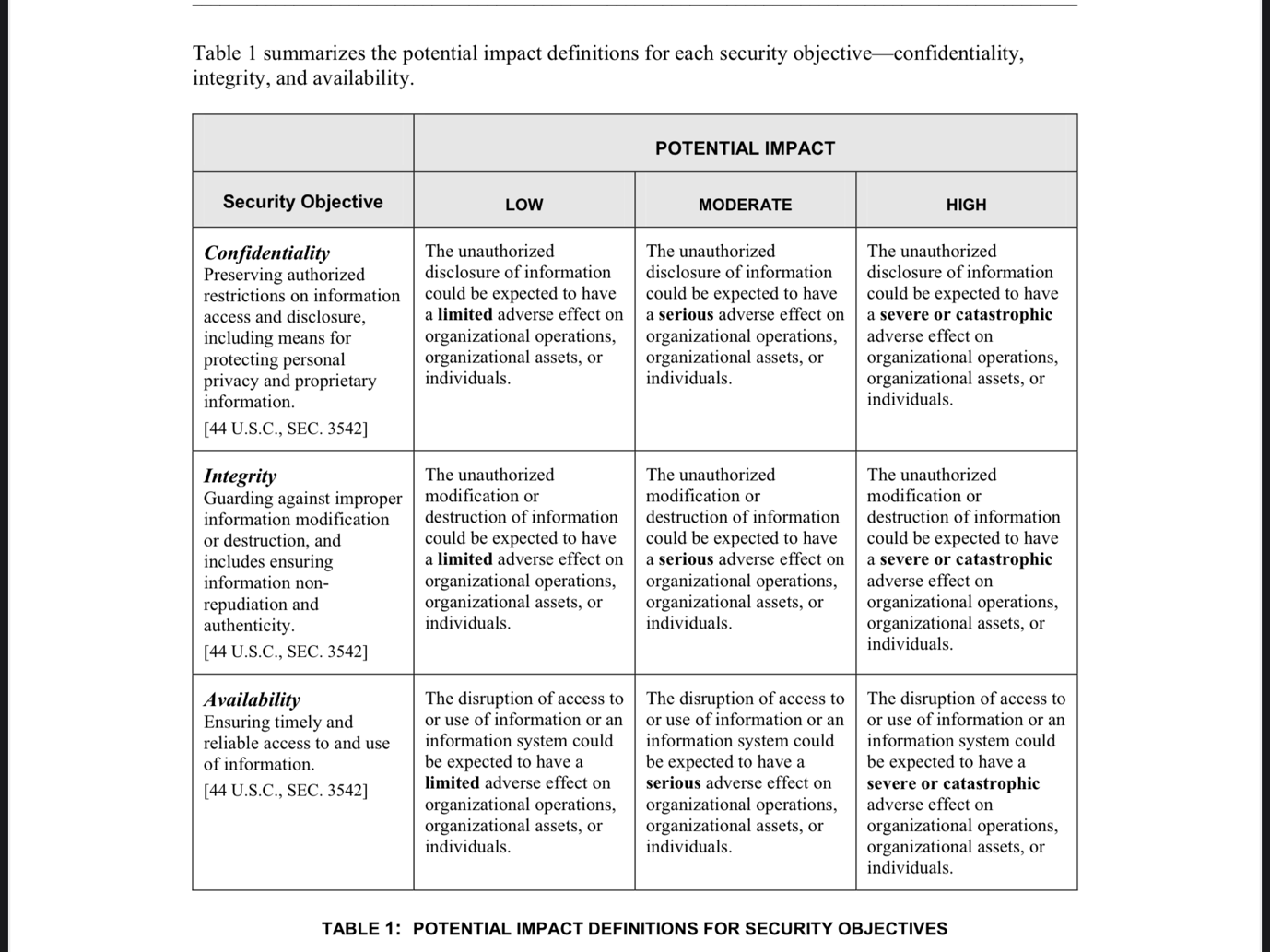
**14. Information System Security Plan Completion Date**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

• Enter the completion date of the plan.

**15. Information System Security Plan Approval Date**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

• Enter the date the system security plan was approved and indicate if the approval documentation is attached or on file.

**Appendix**

**FIPS-199**