Security Assessment Plan Template

[This security assessment plan template was adapted from the FedRAMP Security Assessment Plan (SAP) Template, downloadable here: https://bit.ly/2wAGnZ9.]

1. INTRODUCTION

   [Provide any introductory information here.]

   a. Laws, Regulations, Standards, and Guidance

      [List any relevant laws, regulations, standards, and guidance.]

   b. Purpose

      [Describe the purpose of the assessment.]

2. SCOPE

   a. Information System Names

      [List all target information systems.]

   b. IP Addresses

      [List IP addresses and address ranges in scope.]

   c. Web Applications

      [List target web applications.]

   d. Databases

      [List target databases.]

3. ASSUMPTIONS

   [Identify any assumptions being made prior to conducting the assessment.]

4. METHODOLOGY

[Describe the overall methodology which will be followed to conduct the assessment (how data will be gathered, how security controls will be tested, etc.).]

5. TEST PLAN

    a. Security Assessment Team

        [List members of the assessment team and their contact information.]

    b. Target Organization Points of Contact

        [List names and contact information for members of the organization who should be contacted for questions, access, in the event of incidents, etc.]

    c. Testing Performed Using Automated Tools

        [List any tools used to conduct automated tests.]

    d. Testing Performed through Manual Methods

        [List any manual methods to conduct tests.]

    e. Schedule

        [Provide a detailed schedule of key events, activities, and dates.]

6. RULES OF ENGAGEMENT

    [Disclose any known scanning source IP addresses. Describe what will and will not be included in the tests (i.e., will intrusive testing or social engineering be included).]

    a. End of Testing

        [Describe what constitutes the end of the test and who will be notified when the tests are complete.]

    b. Communication of Test Results

        [Describe how test results will be communicated and to whom.]

    c. Limitation of Liability

        [Describe any limitations of liability.]

d. Signatures

[Signatures of representatives from the testing and target organizations who can authorize security testing.]