| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **PL-4** | RULES OF BEHAVIOR | |
| **PL-4.1**  **PL-4.1.1**  **PL-4.1.2**  **PL-4.1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization establishes the rules that describe information system user responsibilities and expected behavior with regard to information and information system usage;* 2. *the organization makes the rules available to all information system users; and* 3. *the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Security planning policy; procedures addressing rules of behavior for information system users; rules of behavior; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel who are authorized users of the information system and have signed rules of behavior]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-8, AC-20, CA-3, IA-4, PL-2, PS-6, PS-8, SA-5, SA-7, SA-9  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions**  **\*\*See “**[**Assessment Case Overview**](http://csrc.nist.gov/groups/SMA/fisma/assessment-cases-overview.html)**” for selecting, tailoring and executing action steps\*\*** |
|  | | *\*\*Assessment Case Assessor Note:* More convincing evidence (i.e., greater assurance) of correct implementation and operating as intended can be obtained through the assessment case actions by:   1. **Replacing bracketed values in action gathering statements to apply greater rigor in the assessment** (e.g, . replacing [“*reviewing*”] with “*studying*” or “*analyzing*”; replacing [“*observing*”] with “*inspecting*” or “*analyzing*”; replacing [“*basic*”] with “*focused*” or “*comprehensive*”); 2. **Replacing bracketed values in action gathering statements to apply greater sample coverage in the assessment** (e.g, . replacing [“*basic”*] sample with “*focused*” or “*sufficiently large”* sample); 3. **Defining additional action steps to the list of action steps suggested herein that exercise additional test methods** (i.e., Examine, Interview or Test) on additional assessment objects. |
| **PL-4.1.1.1** | | **Examine** security planning policy, procedures addressing rules of behavior, rules of behavior, security plan, or other relevant documents; [*reviewing*] for the rules that describe information system user responsibilities and expected behavior with regard to information and information system usage. |
|  | |  |
| **PL-4.1.2.1** | | **Interview** an agreed-upon [*basic*] sample of information system users; conducting [*basic*] discussions for evidence that the rules identified in PL-4.1.1.1 are available to information system users. |
|  | |  |
| **PL-4.1.3.1** | | **Examine** account management records and signed rules of behavior acknowledgement forms for an agreed-upon [*basic*] sample of information system users; [*reviewing*] for evidence that the organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system. |
|  | | |
| **ASSESSMENT – Control Enhancement 1** | | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | | |
| **PL-4(1)** | | RULES OF BEHAVIOR |
| **PL-4(1).1**  **PL-4(1).1.1**  **PL-4(1).1.1a**  **PL-4(1).1.1b**  **PL-4(1).1.1c** | | **ASSESSMENT OBJECTIVE:**  *Determine if the organization includes in the rules of behavior:*   * *explicit restrictions on the use of social networking sites;* * *posting information on commercial Web sites; and* * *sharing information system account information.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Security planning policy; procedures addressing rules of behavior for information system users; rules of behavior; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel who are authorized users of the information system and have signed rules of behavior]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-8, AC-20, CA-3, IA-4, PL-2, PS-6, PS-8, SA-5, SA-7, SA-9  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **PL-4(1).1.1.1**  **PL-4(1).1.1.1.a**  **PL-4(1).1.1.1.b**  **PL-4(1).1.1.1.c** | | **Examine** rules of behavior; [*reviewing*] for evidence that the rules include:   * explicit restrictions on the use of social networking sites; * posting information on commercial Web sites; and * sharing information system account information. |