| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **AC-22** | PUBLICLY ACCESSIBLE CONTENT | |
| **AC-22.1**  **AC-22.1.1**  **AC-22.1.2**  **AC-22.1.3**  **AC-22.1.4**  **AC-22.1.5**  **AC-22.1.6** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization designates individuals authorized to post information onto an organizational information system that is publicly accessible;* 2. *the organization trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;* 3. *the organization reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system;* 4. *the organization defines the frequency of reviews of the content on the publicly accessible organizational information system for nonpublic information;* 5. *the organization reviews the content on the publicly accessible organizational information system for nonpublic information in accordance with the organization-defined frequency; and* 6. *the organization removes nonpublic information from the publicly accessible organizational information system, if discovered.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing publicly accessible content; list of users authorized to post publicly accessible content on organizational information systems; training materials and/or records; records of publicly accessible information reviews; records of response to nonpublic information on public Web sites; system audit logs; security awareness training records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel responsible for managing publicly accessible information posted on organizational information systems]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-3, AC-6, AT-3, AU-13  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. |
| **AC-22.1.1.1** | | **Examine** access control policy, procedures addressing publicly accessible content, security plan, or other relevant documents; [*reviewing*] for the individuals authorized to post information onto an organizational information system that is publicly accessible. |
|  | |  |
| **AC-22.1.2.1** | | **Examine** access control policy, procedures addressing publicly accessible content, training materials, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to train the authorized individuals identified in AC-22.1.1.1 to ensure that publicly accessible information does not contain nonpublic information. |
| **AC-22.1.2.2** | | **Examine** training records for an agreed-upon [*basic*] sample of individuals authorized to post information onto an organizational information system; [*reviewing*] for evidence that the measures identified in AC-22.1.2.1 are being applied. |
|  | |  |
| **AC-22.1.3.1** | | **Examine** access control policy, procedures addressing publicly accessible content, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to review the proposed content of publicly accessible information for nonpublic information prior to posting onto the information system. |
| **AC-22.1.3.2** | | **Examine** records of publicly accessible information reviews for an agreed-upon [*basic*] sample of information posted on the organizational information system; [*reviewing*] for evidence that the measures identified in AC-22.1.3.1 are being applied. |
| **AC-22.1.3.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for reviewing proposed content of publicly accessible information; conducting [*basic*] discussions for further evidence that the measures identified in AC-22.1.3.1 are being applied. |
|  | |  |
| **AC-22.1.4.1** | | **Examine** access control policy, procedures addressing publicly accessible content, security plan, or other relevant documents; [*reviewing*] for the frequency of reviewing the content on the publicly accessible organization information system for nonpublic information. |
|  | |  |
| **AC-22.1.5.1** | | **Examine** access control policy, procedures addressing publicly accessible content, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to review the content on the publicly accessible organization information system for nonpublic information in accordance with the frequency identified in AC-22.1.4.1 |
| **AC-22.1.5.2** | | **Examine** an agreed-upon [*basic*] sample of records of publicly accessible information reviews; [*reviewing*] for evidence that the measures identified in AC-22.1.5.1 are being applied. |
|  | |  |
| **AC-22.1.6.1** | | **Examine** access control policy, procedures addressing publicly accessible content, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to remove nonpublic information from the publicly accessible organizational information system, if discovered. |
| **AC-22.1.6.2** | | **Examine** information on the publicly accessible information system and an agreed-upon [*basic*] sample of records of publicly accessible information reviews; [*reviewing*] for evidence that measures identified in AC-22.1.6.1 are being applied to remove nonpublic information from the publicly accessible information system, if discovered. |
| **AC-22.1.6.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for managing publicly access information posted on the information system; conducting [*basic*] discussions for further evidence that the measures identified in AC-22.1.6.1 are being applied to remove nonpublic information from the publicly accessible information system, if discovered. |
|  | | |