Group 7 - Assignment 3

AC-1

The organization:

(a) Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:

(1) An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(2) Procedures to facilitate the implementation of the access control policy and associated access controls; and

(b) Reviews and updates the current:

(1) Access control policy [FedRAMP Assignment: at least every 3 years]; and

(2) Access control procedures [FedRAMP Assignment: at least annually].

| AC-1 | Control Summary Information |
| --- | --- |
| Responsible Role: **Chief Information Security Officer (CISO)** | |
| Parameter AC-1(a):  The policy is disseminated to **the** **security team, IT department, compliance officers, and all relevant business unit managers.** | |
| Parameter AC-1(b)(1):  The access control policy shall be reviewed and updated **at least every 3 years.** | |
| Parameter AC-1(b)(2):  The access control procedures shall be reviewed and **updated at least annually.** | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  **X**  Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  **X**  Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific) | |

| AC-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The purpose of this access control policy is to ensure that access to SecureGovTransfer’s information system and data is strictly controlled and restricted to only those who have a need to know. This policy applies to all employees, contractors, and third parties who access SecureGov Transfer’s system and data. The CISO owns and enforces this policy and the Director of Cybersecurity manages and enforces the access controls. The IT system administrators implement and maintain the access controls on the systems. The compliance officers ensure that access control measures meet the appropriate requirements of FEDRAMP at the moderate level. Business unit managers are responsible to ensure the measures outlined in this document are followed within their units.  The business unit leaders and management is committed to supporting and enforcing this access control policy as it is outlined herein. Regular coordination is maintained between IT, Security, Compliance, and all business units to ensure measures are effective and align with business needs and requirements.  Accounts shall only be created upon a successful approval of an access request which is submitted through a formal process using the designated form. The access requests are reviewed and approved by the appropriate business unit manager and the Director of Cybersecurity. All approved access requests are documented.  Roles shall be defined based on job functions and are logically organized based on specific access rights. Users are assigned roles based on their job responsibilities and regular audits shall be performed to ensure they align with the user’s current job function.  Procedures are in place to detect and respond to access control incidents. When an access control incident is detected, it shall be investigated quickly and the appropriate actions are taken to mitigate any risk that is associated. All access control incidents shall be reported to the CISO, the Director of Cybersecurity, and the appropriate business unit manager. |
| Part b1 | A review of the access control policy is to be conducted at least once every 3 years by the CISO or his/her designate. The responsible party shall schedule a policy review meeting and notify those who have been given the policy. The team assesses the current access control policy against the latest regulatory requirements, any relative audit findings, changes in standards, and recent organizational changes. Based upon the review, the CISO drafts the updates to the access control policy. The draft is then sent to the review team for feedback. Upon the delivery of feedback, the CISO adds the appropriate changes and then sends the policy to senior management for approval. Upon formal approval, the updated policy is disseminated to the security team, IT department, compliance officers, and all relevant business unit managers. |
| Part b2 | A review of the access control procedures shall be conducted at least annually by the Director of Cybersecurity. The meeting is scheduled and a notification is sent to those who have been given the procedures previously. The review team assesses the current procedures for effectiveness and compliance. Feedback from users on inefficiencies or procedural issues is incorporated as appropriate. Findings from previous audits are looked at to determine any gaps or weaknesses. Based on this review, the Director of Cybersecurity drafts the updates and sends it to the review team for review and feedback. The group feedback is incorporated into the procedure document and then it is sent to the CISO for approval and formal sign off. After the CISO has officially signed off on the new procedures, they are disseminated to the security team, IT department, compliance officers, and all relevant business unit managers |

AT-1

The organization:

(a) Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:

(1) A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(2) Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and

(b) Reviews and updates the current:

(1) Security awareness and training policy [FedRAMP Assignment: at least every 3 years]; and

(2) Security awareness and training procedures [FedRAMP Assignment: at least annually].

| AT-1 | Control Summary Information |
| --- | --- |
| Responsible Role: **Chief Information Security Officer (CISO)** | |
| Parameter AT-1(a): a policy that will apply to **the** **security team, IT department, compliance officers, and all relevant business unit managers.** | |
| Parameter AT-1(b)(1): The org shall review and update this material **every three years** | |
| Parameter AT-1(b)(2): The org will update and review security procedures **annually** | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  **X** Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  **X** Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific) | |

| AT-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The purpose of this policy is to ensure that employees are up-to-date on all security awareness and security training. This policy applies to all staff members within the organization. The CISO owns this policy and ensures that all staff members within the organization are following said policy.  All department managers are responsible for making sure their staff members follow this policy and are caught up to date on all security training. In addition, managers need to make sure that they are putting up awareness posters/flyers/sending emails/etc. in relation to this policy  The training will inform employees about policies related to security awareness. Meetings must happen at least twice a year to keep up with current security trends. This will be led by the training department, and a member of the security team. Emails should be sent at least once every two weeks, with high-level overviews of current security awareness material. Logs of those who have completed the training must be kept for at least 5 years before they can be discarded.  Security awareness material needs to contain information that is current and relevant to the organization and the cybersecurity landscape. The cybersecurity team will be in charge of designating what is current and what should be focused on in the emails and training. |
| Part b | A review of this security awareness and training is to be conducted at least once every 3 years by the CISO or his/her designate. The responsible party shall schedule a training review meeting and notify those given the training. The team assesses the current training content against the latest regulatory requirements, any relative audit findings, changes in standards, and recent organizational changes. Based on the review, the CISO drafts the updates to the policy. The draft is then sent to the review team for feedback. Upon feedback delivery, the CISO adds the appropriate changes and then sends the training to senior management for approval. The updated policy is disseminated upon formal approval to the security team, IT department, compliance officers, and all relevant business unit managers. |
| Part b2 | The Security Awareness and Training policy shall be reviewed and updated as needed at least annually. The review process shall be conducted by the Director of Cybersecurity but include input from the review team which shall consist of the security team, members of the IT department, and compliance officers. The review will include evaluating the effectiveness of the current security awareness and training, any areas for improvement, suggestions for improvement by business unit leaders, and any previous feedback on effectiveness and topics to be covered. Updates shall be made according to what was discovered through the review process. The procedures shall be revised and reviewed by the Director of Cybersecurity and the review team. Once the revisions have been completed and signed off, it will be sent to the CISO for final approval. Upon final approval, the new training and awareness programs will be disseminated to the appropriate parties. |

AU-1

The organization:

(a) Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:

(1) An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(2) Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and

(b) Reviews and updates the current:

(1) Audit and accountability policy [FedRAMP Assignment: at every 3 years]; and

(2) Audit and accountability procedures [FedRAMP Assignment: at least annually].

| AU-1 | Control Summary Information |
| --- | --- |
| Responsible Role: **Chief Information Security Officer (CISO)** | |
| Parameter AU-1(a): The policy that will apply to **the** **security team, IT department, compliance officers, and all relevant business unit managers.** | |
| Parameter AU-1(b)(1): The org shall review and update the audit and accountability material **every three years.** | |
| Parameter AU-1(b)(2): The org will update and review the audit and accountability procedures **annually.** | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  **X** Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Origination (check all that apply):  **X** Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific) | |

| AU-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The purpose of this policy is to ensure that employees are able to conduct audits in a manner approved by the company, in addition, this policy will establish how accountability will be recorded, stored and used within the organization. This policy applies to all staff members within the organization. The CISO owns this policy and ensures that all staff members within the organization are following said policy.  The CISO will be responsible for delegating a team to conduct audits when requested by an employee of the organization. The team will either directly report to the CISO or a manager appointed by the CISO.  This policy will serve to make sure all audits and accountability within the organization are uniform throughout all departments. It will also serve to help make a standard for all future audits so there is no difference between what was and was not audited.  Event logs will be enforced on all information systems including critical system events, failed login attempts, data access, system changes, and security incidents. These logs shall be retained for a minimum of ninety days or as outlined in regulatory requirements. Logs shall be collected in real time and stored within a central syslog server. Access to these logs shall be restricted to authorized personnel only. Logs shall be written in a “write once read many” (WORM) method and encrypted at rest and in transit.  Reviews of logs shall be done on a regular weekly basis to identify any suspicious activity or potential incidents. Automated alerts are configured to notify the internal security operations center. Activity that is deemed as suspicious or abnormal shall be investigated for further analysis and investigation. If the activity is deemed as an incident, incident response procedures shall be enacted.  Audit trails are maintained for all critical system actions to maintain a record of these activities. These trails are protected against tampering and any unauthorized access via access controls. These audit trails are reviewed at least weekly to ensure their completeness and integrity. |
| Part b1 | A review of the audit and accountability policy shall be conducted at least once every 3 years by the CISO or his/her designate. A policy review meeting shall be held by the responsible party in which they shall assess the current audit and accountability policy against the latest regulatory requirements and update the policy and controls as necessary to ensure they remain effective, relevant, and compliant with the current standards and regulations. A plan to address any identified gaps or deficiencies in the audit and accountability controls will be formulated. Upon completion of the policy review meeting, a draft of appropriate changes shall be sent to senior management for approval. Upon formal approval, updated policies shall be disbursed to the security team and all relevant personnel. |
| Part b2 | The audit and accountability procedures shall be reviewed and updated as needed at least annually. The review process shall be conducted by the Director of Cybersecurity but include input from the review team which shall consist of the security team, members of the IT department, and compliance officers. The review will include evaluating the effectiveness of the current audit and accountability procedures, any areas for improvement, suggestions for improvement by business unit leaders, and any previous audit findings. Updates shall be made according to what was discovered through the review process. The procedures shall be revised and reviewed by the Director of Cybersecurity and the review team. Once the draft has been completed and signed off, it will be sent to the CISO for final approval. Upon final approval, the new procedures will be disseminated to the appropriate parties. |