**AC-1 ACCESS CONTROL POLICY AND PROCEDURES**

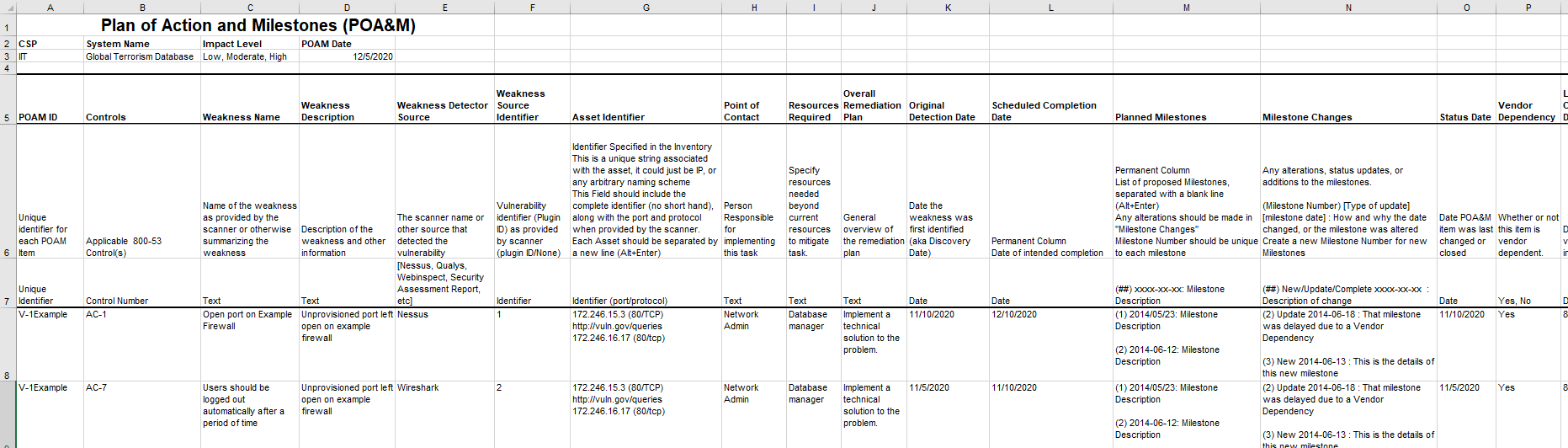
The organization will -

* This organization addresses that the Administrator has all permissions to enter, modify, and delete any data inputted in to the database.
* Database administrators are responsible for upholding the integrity of the database and network administrators are responsible for ensuring that user names and passwords are giving to correct personnel based on role.
* The testing account is only given the minimum permissions of reading to ensure that any non faculty member that gains access to the account can not edit the database.
* Each user created account will have permission to only read data and must be protected with a password.
* Make sure roles are assigned to a database to ensure that all personnel are only able to modify the scope of their permissions listed above.

**CA–5 PLAN OF ACTION AND MILESTONES**

The organization will –

* Develop a plan of action and milestones for the information system
* Document the organization’s planned remedial actions
* Correct any weaknesses or deficiencies noted during assessment
* Reduce or eliminate any known vulnerabilities in the system from the time of assessment
* Update the plan of action and milestones automatically when any new findings are made from assessments



**CA-7 CONTINUOUS MONITORING**

The organization will –

* Establish that all personnel including admins will be monitored to ensure database integrity by network admin
* Establish that any queries, log-in attempts, and log in information will be monitored to ensure that any personnel will not attempt to download the data off the server.
* Log files will be automatically monitored for any activity deemed suspicious by the organization.
* Any suspicious findings will be investigated by the organization and if deemed dangerous, immediate suspension of inside personnel or outside investigations will be conducted.

PL-2 SYSTEM SECURITY PLAN

The organization will –

* Ensure that system protocols are up to date
* Ensure that any malicious code will not be authorized to run on the database
* Ensures that the database can not be copied to an outside source
* Ensure that all personnel are kept up to date with any new security policies
* Describes the operational environment for the information system
* Communicate any changes to security plan to all essential personnel
* Ensure that security plan is only sent to those with proper authorization
* Review the security plan for any information about the system

**CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES**

The organization will –

* Develop, document, and disseminate information of the contingency policy to all personnel
* Create a contingency planning policy that addresses the purpose, scope, roles, and responsibility during a contingency
* Also address coordination among other organizational entities and compliance between the entities
* Develop procedures to facilitate the implementation of the contingency planning policy and controls
* Review and update the current contingency planning policies and procedures

**CP-2 CONTINGENCY PLAN**

The organization will-

* Develop a contingency plan
* Identify the essential missions and business functions such as maintenance of data and databases
* Recover any data that is lost in the database that occurred after 2000, and ensure that all of that priority is reserved for that data
* Ensure all management and decision making is made and reviewed by the CISO
* Ensure that the contingency plan is updated on a yearly basis to include any new discoveries and reviewed by personnel
* Only be distributed to essential personnel with a security clearance deemed by the organization
* Ensures that contingency plans are communicated in a concise fashion to upper management and all personnel handling the database management.

**CP-3 CONTINGENCY TRAINING**

The organization provides contingency training information based on role:

* Users: training on need to understand when and where to report for duty during contingency operations
* System administrators: training on how to set up information systems at alternate processing and storage site
* Managers/Senior leaders: “Training on how to conduct mission essential functions in designated off site locations and how to establish communications with other governmental entities for purposes of coordination on contingency related activities” (NVD-Rev4, 2020)
* Database architects: Training on which data to prioritize on recovery and how to restore data to original state

**CM-11 USER-INSTALLED SOFTWARE**

The organization will-

* Not allow any software to be downloaded by users without the permission of the network administrator
* Automatically rollback any software that is downloaded at the end of the user session
* All software installation policies will be monitored by the network administrator and enforced by the admin managers
* Any other software guidelines will be enforced by using SANS User Installation Software guidelines: <https://www.sans.edu/student-files/projects/200711_002.pdf>

**PE-12 EMERGENCY LIGHTING**

The organization will -

* employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

## **IA-1 IDENTIFICATION & AUTHENTICATION POLICY AND PROCEDURES**

The organization will –

* Develop an identification and authentication policy
* Address purpose, scope, roles, and responsibilities within the policy
* Also address any procedures to facilitate the implementation of the identification and authentication policy
* Develop a strategy to minimize the risk within the organization

**IR-4 INCIDENT HANDLING**

The organization will –

* Handle all incidents through an automated ticketing system within the organization
* Monitor all network traffic through Wireshark and various methods through the network administrator
* Focus data recovery on all data past year 2000 if a data incident were to occur
* Ensure that in the event of any incidents, the proper measures are taken to handle the preparation, containment, eradication, and recovery of any necessary data

**IR-5 INCIDENT MONITORING**

The organization will –

* Document and track any system security incidents
* Maintain any records about the status, time, type of the incident and any other information necessary
* Evaluate any incident details
* Retrieve any information about incidents from the various incident handling procedures

**IR-6 Incident Reporting**

The organization will –

* Report any incidents to the incident response team and any essential personnel within 1 week of the incident
* Report any incident information directly to the senior database managers and senior network administrators
* The senior managers and network administrators will report any security incident to the US-CERT within one day of receiving the information

**MA-1 System Maintenance Policy and Procedures**

The organization will –

* Create a system maintenance policy
* Address the purpose, scope, roles, and responsibilities in the policy
* Create procedures to facilitate the implementation of the system maintenance policy and controls
* Review and update the current system maintenance policy and procedures

**SA-2 Allocation of Resources**

The organization will-

* Allocate at least $10,000 for the hosting of the database servers and at least $500,000 to pay for the personnel to manage the database and information system
* Keep a team of at least 5 people in each department that are paid to manage the network, database, and security of the system.
* Allocate at least $80,000 each for all personnel on teams to be paid for their work of managing and monitoring the system
* Allocate $60,000 of spare funds for the development of another database if necessary

**SI-12 INFORMATION HANDLING AND RETENTION**

The organization will –

* Handle and retain information within the database and network in according with federal law, executive order, and any policies
* Maintain information and any records in accordance to the National Archives and Records Administration guidelines

**PE-13 FIRE PROTECTION**

The organization will –

* Ensure that building is following proper fire safety protocols
* Ensure that any fire suppression and fire detection devices are supported by the system and working properly
* Any location with access to data will have the proper fire suppression and detection devices installed and have preventative fire measures available inside the room such as fire extinguishers

**References**

All information cited from

NVD - Rev4. (2020). Retrieved 5 December 2020, from https://nvd.nist.gov/800-53/Rev4/impact/low