SECURITY ASSESSMENT AND AUTHORIZATION POLICY

**SCOPE:**

This security assessment policy servers as the universal foundation for information security for this database, final\_database. This policy will be set up as the standard for information security as required by NIST. It befalls on the database administrator to establish the set of standards for information security to maintain the security, and integrity of the distributed information technology. This policy will be directly linked to any user or personnel, regardless of level in the company, who interacts with the information system on behalf of the organization. Any entity operating within the organization is responsible for abiding and following the guidelines to use this document.

This document provides security policy statements for the security assessment and authorization process for the usage and management of logical access to information systems and data (final\_database) of which is owned and operated by the organization.

**RESPONSIBILITIES:**

Personal roles for the company are to be outlined below and the role served by each entity with the security and authorization for keeping the compliance and maintenance. Roles are defined to ensure information s access is given to the relevant individuals who are deemed as relevant.

|  |  |
| --- | --- |
| Name of Role | Responsibility/Definition |
| Risk Management Officer | Communicating risk policies to the organization. Creating hands-on training for it also. Must ensure that the security safeguards and controls are created and are working as their intended function. Must constantly review the risk management policies and keep them up to day. . |
| Agency Management | The designated organization officials who are to approve all the operations carried out by the organization in regards to the information system. In charge of constant moderation and development of the assessment and authorization program. |

**POLICY:**

All the assets that fall under the scope of the organization must be meeting the security controls as outlined in NIST SP-800-53, security privacy and controls. The purpose of the authorization and assessment process is in regards to keeping compliance with the information security policies. Such policies will be critical in reducing the risk of breaches occurring and the mitigation of the potential of any ones in the future. Assessments will be carried out to determine the reliability of the current controls implemented correctly. The content to be tested is that these controls are working as intended, and creating the expected results that align with the security requirements of the organization’s information system. **Authorization** is given to the relevant users who are granted access to carry out operations on the information systems over a window of time. This access also comes with accepting the risk in letting users into the system.

All access and authorization to the information systems are to be predetermined by the management from who can access it through the mediums on which they can be accessed. These authorized systems extend as far: workstations, servers, devices, location, and network repositories. It's the intended usage of this document to outline the assessment and the process for the authorization for ensuring the best security practices to keep the integrity of the information systems.

The document created “Security Assessment and Authorization”, is meant to establish NIST’s 800-53. Serving as the official policy for all inquiries and questions made in regards to the security domain of the organization. This document should be reviewed and renewed bi-annualy to ensure that the best and latest security practices are being followed.

**SYSTEM INTERCONNECTIONS SECURITY:**

This section has been done with accordance by the standards of NIST Special Publications 800-47 Security Guide for Interconnecting Information Technology Systems. This section will be reviewed by the administration committee on a yearly basis.

The National Institute of Technology and Standards defines *system interconnections* when two individual information technology, or IT, systems are directly connecting and sharing any type of information. Any changes being passed on, or modifications are to be documented as per the guidelines outlined in the Interconnection Security Agreement (ISA) of the organization.

All IT systems of the organization must meet all the requirements to be eligible for authorizing connections to other IT systems. They will have to maintain and execute the following functions:

* Execute connections that follow the guidelines of the Interconnecting Security Agreements.
* Documentation on: security breaches, security requirements, incident handling, roles, the information being transferred.
* Creation of a specification of all systems being blacklisted by default, and only the specified systems being allowed access to the database.
* Specific procedure for carrying out connections:
  1. Approval from the database administrator as a sign agreement on paper or electronically signed
  2. Making a request for connection to the IT administrator to grant access. On the request the following must be specified:
     + Reason for connecting
     + The type of connecting required
     + Personnel who are going to be involved in the connection
     + The time frame needed for having access to the system
     + The information being accessed
  3. Personnel who will be responsible for the system interconnection are responsible for providing a **risk management** and risk impact assessments.
  4. Updates to the ISA as vulnerabilities come to surface,
     + There will still be the yearly reviews, but any problems with the system should be constantly monitored and updated as needed
  5. Termination of session once having expired

**Control Enhancements (1):**

**RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS (MODERATE CONTROL):**

For all data within the system that falls under “*Restricted Data”* will have its own guidelines and standards, for being accessed by external parties or information systems. Just as the previous system this standard will consist of a blacklist policy of denying all connections made or attempted. The strongest policy standard will be applied to this to ensure the security of this higher tier data.

**SECURITY AUTHORIZATION:**

1. For each of the individual information systems that exists within the organization they will each be overseen by a system administrator or senior management. This entity will be responsible for:

* Verification that the employee’s being overseen are following the best practices protection of the information system.
* Information System meeting all standards imposed by the company and the government.
* Yearly compliance on the system being fulfilled and documented.
* Employees or personnel granted access to undergo yearly review to ensure that they are not leaking or disclosing any sensitive information.

1. Before any system operation is done on the information system Authorization To Operate must be granted.
   1. All the employees or users interacting with the system must ensure that any of their action does not violate the segregation controls. This includes:
      1. Disk Cleanup,
      2. Disk Fragmentation, or
      3. Disk Archival
   2. Before any of these can take place they must be granted authorization.
   3. If authorization is granted and it violates the segregation controls, the organization is responsible for listing precautions to prevent such an event.
   4. This precaution could consist of close auditing for confidence in assurance and action taken.
2. Documentation must be done on the system as a whole. It reflecting any changes done on:
   1. App,
   2. Data Structure, or
   3. Authorization changes
3. Any access that is successfully granted must be tied with:
   1. A window of expiration
   2. Authentication of identity
   3. Access Rights

**CONTINUOUS MONITORING:**

The organization will be responsible for the implementation and maintenance of a program for the continuous monitoring of the system. This program will be responsible for keeping track of these three variables:

* Metrics
* Rate of Assessments
* Reports related to Security

This monitoring will encompass both the physical and the cloud base of the database. As both of these are as important for the organization.

The organization has the duty of conducting annual security audits on all of the information systems. Alongside security there will also be a risk assessment to assess the current state of the environment.

Requirements for this program:

* A management system for the system and its components
* Capable of measuring the risk associated with the environment
* Security controls;
  + Scheduled scans on the system
  + Criteria for supporting documentation
  + Compliance expectations
  + Security Reports/Results
* All operators of the information system are responsible for still following the specified guidelines and expectations.
  + Analyze security at all levels and identify biggest weakness at each perspective level
  + Reporting of security status to their administrator
* Demonstration of continuous monitoring being performed and implemented across all levels of the organization.
  + Security
  + Availability
  + Integrity

**INTERNAL SYSTEM CONNECTIONS:**

Security compliance is expected to be done on the devices that the information systems are connecting to. (intra-system connections)

This list can include the following:

* Computers of any sort
* Mobile devices
* Smart Devices (Internet of Things)
* Printers/Copiers/Fax Machines
* Servers

Any device capable of holding, storing data or capturing is expected to meet the specified baseline configurations.

The System Administrator has the duty of the following:

* Creation of classes of components that are allowed for internal connections in the information system.
* Establishing the baseline configurations for each of the classes specified
* Defining the defining characteristics of the security system for these classes. Thesy can be specified as the following
  + Low
  + Moderate
  + High
* Each of these being related to the FIPS-199 categorization

**VIOLATION & ENFORCEMENT:**

Failure by any party to comply with the following guidelines or expectations can result in legal action of the accused. Any entity breaking this will result in their termination and prosecutions to the highest extent of the law.

Approved by: Illinois Institute of Technology - Database Concepts with SQL ITM82