**DATABASE SPECIFICATIONS**

**TABLE OF CONTENTS**

Page #

1. GENERAL INFORMATION

1.1 Purpose 6

1.2 Scope

1.3 System Overview

1.4 Project References

2.0 ACCESS CONTROLS 7

2.1 Policy and Procedures

2.2 Controls implemented

2.3 AC-1: ACCESS CONTROL POLICY AND PROCEDURES

2.4 AC-2: ACCOUNT MANAGEMENT

2.5 AC-3: ACCESS ENFORCEMENT

2.6 AC-7: UNSUCCESSFUL LOGON ATTEMPTS

2.7 AC-8: SYSTEM USE NOTIFICATION

3.0 AUDIT AND ACCOUNTABILITY 8

3.1 Policy and Procedures

3.2 Controls implemented

3.3 AU-1: AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

3.4 AU-2: AUDIT EVENTS

3.5 AU-3: CONTENT OF AUDIT RECORDS

3.6 AU-4: AUDIT STORAGE CAPACITY

3.7 AU-5: RESPONSE TO AUDIT PROCESSING FAILURES

3.8 AU-6: AUDIT REVIEW, ANALYSIS, AND REPORTING

3.9 AU-8: TIME STAMPS

4.0 PERSONNEL SECURITY 9

4.1 Policy and Procedures

4.2 Controls implemented

4.3 PS-1: PERSONNEL SECURITY POLICY AND PROCEDURES

4.4 PS-2: POSITION RISK DESIGNATION

4.5 PS-3: PERSONNEL SCREENING

4.6 PS-4: PERSONNEL TERMINATION

4.7 PS-5: PERSONNEL TRANSFER

4.8 PS-6: ACCESS AGREEMENTS

4.9 PS-7: THIRD-PARTY PERSONNEL SECURITY

4.10 PS-8: PERSONNEL SANCTIONS

5.0 RISK ASSESSMENT 10

5.1 Policy and Procedures

5.2 Controls implemented

5.3 RA-2: SECURITY CATEGORIZATION

5.4 RA-3: RISK ASSESSMENT

5.5 RA-5: VULNERABILITY SCANNING

6.0 IDENTIFICATION AND AUTHENTICATION 11

6.1 Policy and Procedures

6.2 Controls implemented

6.3 IA-4: IDENTIFIER MANAGEMENT

6.4 IA-5: AUTHENTICATOR MANAGEMENT

6.5 IA-6: AUTHENTICATOR FEEDBACK

7.0 SYSTEM AND COMMUNCATIONS PROTECTION 12

7.1 Policy and Procedures

7.2 Controls implemented

7.3 SC-1: SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND

PROCEDURES

7.4 SC-7: BOUNDARY PROTECTION

7.5 SC-13: CRYPTOGRAPHIC PROTECTION

7.6 SC-15: COLLABORATIVE COMPUTING DEVICES

7.7 SC-20: SECURE NAME / ADDRESS RESOLUTION SERVICE

(AUTHORITATIVE SOURCE)

8.0 SYSTEM AND INFORMATION INTEGRITY 13

8.1 Policy and Procedures

8.2 Controls implemented

8.3 SI-2: FLAW REMEDIATION

8.4 SI-3: MALICIOUS CODE PROTECTION

8.5 SI-4: INFORMATION SYSTEM MONITORING

8.6 SI-5: SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

**Revision 4 Sheet**

|  |  |  |
| --- | --- | --- |
| **No.** | **Date** | **Controls Description** |
| AC-1 | 11/30/20 | ACCESS CONTROL POLICY AND PROCEDURES |
| AC-2 | 11/30/20 | ACCOUNT MANAGEMENT |
| AC-3 | 11/30/20 | ACCESS ENFORCEMENT |
| AC-7 | 11/30/20 | UNSUCCESSFUL LOGON ATTEMPTS |
| AC-8 | 11/30/20 | SYSTEM USE NOTIFICATION |
| PS-1 | 11/30/20 | PERSONNEL SECURITY POLICY AND PROCEDURES |
| PS-2 | 11/30/20 | POSITION RISK DESIGNATION |
| PS-3 | 11/30/20 | PERSONNEL SCREENING |
| PS-4 | 11/30/20 | PERSONNEL TERMINATION |
| PS-5 | 11/30/20 | PERSONNEL TRANSFER |
| PS-6 | 11/30/20 | ACCESS AGREEMENTS |
| PS-7 | 11/30/20 | THIRD-PARTY PERSONNEL SECURITY |
| PS-8 | 11/30/20 | PERSONNEL SANCTIONS |
| RA-2 | 11/30/20 | SECURITY CATEGORIZATION |
| RA-3 | 11/30/20 | RISK ASSESSMENT |
| RA-5 | 11/30/20 | VULNERABILITY SCANNING |
| AU-1 | 11/30/20 | AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES |
| AU-2 | 11/30/20 | AUDIT EVENTS |
| AU-3 | 11/30/20 | CONTENT OF AUDIT RECORDS |
| AU-4 | 11/30/20 | AUDIT STORAGE CAPACITY |
| AU-5 | 11/30/20 | RESPONSE TO AUDIT PROCESSING FAILURES |
| AU-6 | 11/30/20 | AUDIT REVIEW, ANALYSIS, AND REPORTING |
| AU-8 | 11/30/20 | TIME STAMPS |
| IA-4 | 11/30/20 | IDENTIFIER MANAGEMENT |
| IA-5 | 11/30/20 | AUTHENTICATOR MANAGEMENT |
| IA-6 | 11/30/20 | AUTHENTICATOR FEEDBACK |
| SC-20 | 11/30/20 | SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) |
| SC-15 | 11/30/20 | COLLABORATIVE COMPUTING DEVICES |
| SC-13 | 11/30/20 | CRYPTOGRAPHIC PROTECTION |
| SC-1 | 11/30/20 | SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES |
| SC-7 | 11/30/20 | BOUNDARY PROTECTION |
| SI-3 | 11/30/20 | MALICIOUS CODE PROTECTION |
| SI-4 | 11/30/20 | INFORMATION SYSTEM MONITORING |
| SI-2 | 11/30/20 | FLAW REMEDIATION |
| SI-5 | 11/30/20 | SECURITY ALERTS, ADVISORIES, AND DIRECTIVES |

1. GENERAL INFORMATION

## 1.1 Purpose

The purpose of this database is to capture crimes and/or nefarious acts that can range from physical crimes, terrorist attacks, criminal attacks, and more globally.

## 1.2 Scope

The Database Specifications outlines the low-impact controls implemented within the database, and its effect on the user(s) as well as the database itself.

## 1.3 System Overview

The database created by Enrique Budiono, Youdi Chen, and Grace Sopha is a SQL-based structure ran on a Debian operating system. The twenty tables that comprise the database consists of countries ranging from anywhere between North America, South America, Europe, Africa and Asia. Countries included, but not limited to, are Japan, United Kingdom, Indonesia, West Germany, Ethiopia and several more. As stated, it will pull information of the crimes and misconducts recorded around the globe. This database is currently under development and undergoing modifications.

## 1.4 Project References

* Global Terrorism Database (<https://start.umd.edu/gtd/>)
* National Vulnerability Database (<https://www.nist.gov/>)

1. ACCESS CONTROLS

## 2.1 Policy and Procedures

Access controls are best defined as who and what has specified entrance to the database. The policy reflects any federal laws, executive orders, directives, rules and regulations, and guidance. Responsibilities of the access control include roles, responsibilities, management commitment, coordination, and compliance.

## 2.2 Controls Implemented

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

The user is able to view their grants, as well as what portions and actions they are allowed to execute while using the database.

**2.4 AC-2: ACCOUNT MANAGEMENT**

The accounts created within the database are organized depending on what access and roles they hold within the system. Primarily, this control is used to manage individual or group accounts and their privileges.

**2.5 AC-3: ACCESS ENFORCEMENT**

The system enforces an automated system that will only allow users to execute what their account allows them to.

**2.6 AC-7: UNSUCCESSFUL LOGON ATTEMPTS**

The system will only allow registered accounts to access the database and initiate a lock when the password is not correct.

**2.7 AC-8: SYSTEM USE NOTIFICATION**

Upon login, the system will display a message and/or banner that outlines the rules and regulations required to use the database.

1. AUDIT AND ACCOUNTABILITY

## 3.1 Policy and Procedures

Audit and accountability regulate and overlooks what occurrences are happening within the database. The policy reflects any federal laws, executive orders, directives, rules and regulations, and guidance. Responsibilities of the audit and accountability control include facilitation, roles, responsibilities, management commitment, coordination, and compliance.

## 3.2 Controls Implemented

**3.3 AU-1: AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES**

The user is able to view what actions are to be facilitated by the audit while using the database.

**3.4 AU-2: AUDIT EVENTS**

The system will oversee any audit events that have a relation to the security of the information within the database. This includes password changes, failed logins, etc.

**3.5 AU-3: CONTENT OF AUDIT RECORDS**

The system storages the audit records according to timestamps, source, destinations, etc.

**3.6 AU-4: AUDIT STORAGE CAPACITY**

The system will maintain a feasible storage capacity for its audit records and warn the user of the capacity being reached.

**3.7 AU-5: RESPONSE TO AUDIT PROCESSING FAILURES**

If the system has bugs or any mishaps within the software, the audit which deals with failing processes is to document those incidents.

**3.8 AU-6: AUDIT REVIEW, ANALYSIS, AND REPORTING**

The system will analyze its records of audits and report any significance that needs to be fixed.

**3.9 AU-8: TIME STAMPS**

The system uses its internal clock to track audits that are documented.

1. PERSONAL SECURITY

## 4.1 Policy and Procedures

Personal security protects the users as well as the information that is stored in the database. The policy reflects any federal laws, executive orders, directives, rules and regulations, and guidance. Responsibilities of the access control include roles, responsibilities, management commitment, coordination, and compliance.

## 4.2 Controls Implemented

**4.3 PS-1: PERSONNEL SECURITY POLICY AND PROCEDURES**

The user is able to view what processes/screenings are required in order for them to be able to access the database.

**4.4 PS-2: POSITION RISK DESIGNATION**

The system assigns risk designation to all positions within the organization, which allows the user guidance.

**4.5 PS-3: PERSONNEL SCREENING**

The system will automatically screen each individual who accesses the database.

**4.6 PS-4: PERSONNEL TERMINATION**

When a user is expelled from the system, an exit interview is put in place, so the terminated user is aware of any security constraints that comes from usage.

**4.7 PS-5: PERSONNEL TRANSFER**

When a terminated user is returning old keys/logins, the system records whoever the new keys/passes are transferred to, as well as the history of use.

**4.8 PS-6: ACCESS AGREEMENTS**

Before use, the user agrees to any NDAs, terms of service, rules, etc.

**4.9 PS-7: THIRD-PARTY PERSONNEL SECURITY**

Third-party organizations may have rights to oversee security of database.

**4.10 PS-8: PERSONNEL SANCTIONS**

If a user fails to comply, the system will place a formal sanction on the user.

1. RISK ASSESSMENT

## 5.1 Policy and Procedures

Risk assessment is the analysis of what factors can pose a threat to the security of the database. The policy reflects any federal laws, executive orders, directives, rules and regulations, and guidance. Responsibilities of the access control include roles, responsibilities, management commitment, coordination, and compliance.

## 5.2 Controls Implemented

**5.3 RA-2: SECURITY CATEGORIZATION**

The system is to place authorization boundaries, which allows it to categorize the information system into “security categories”. This can store items such as loss of confidentiality, assets, impacts, etc.

**5.4 RA-3: RISK ASSESSMENT**

The system will run assessments that analyze the threats from within and outside of database. It takes vulnerabilities, likeliness of attack, impacts to organization, etc. into account, then detects what factor can be harmful.

**5.5 RA-5: VULNERABILITY SCANNING**

The system’s security categorization maintains the frequency of the scans for all components of the information system. This includes regularly checking sources such as printers, fax, etc.

1. IDENTIFICATION AND AUTHENTICATION

## 6.1 Policy and Procedures

Identification and authentication ensure that all users and devices that connect to the database are allowed to be there. The policy reflects any federal laws, executive orders, directives, rules and regulations, and guidance. Responsibilities of the access control include roles, responsibilities, management commitment, coordination, and compliance.

## 6.2 Controls Implemented

**6.3 IA-4: IDENTIFIER MANAGEMENT**

The system will be able to track items such as media access control, IP address, etc. and grant access based on identifying features that comply with the database.

**6.4 IA-5: AUTHENTICATOR MANAGEMENT**

The system will only allow access with specific keys and passes are used. This includes passwords, biometrics, key cards, etc.

**6.5 IA-6: AUTHENTICATOR FEEDBACK**

The system is automatically set to protect from non-authorized users’ access. Passwords may appear in asterisk or hashes to protect from shoulder-surfing and hacking.

1. SYSTEM AND COMMUNCATIONS PROTECTION

## 7.1 Policy and Procedures

System and communication protection is put in place in order to facilitate user activity, and shield from any potential threats. The policy reflects any federal laws, executive orders, directives, rules and regulations, and guidance. Responsibilities of the access control include roles, responsibilities, management commitment, coordination, and compliance.

## 7.2 Controls Implemented

**7.3 SC-1: SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES**

The user is able to see what activities will be monitored while on database.

**7.4 SC-7: BOUNDARY PROTECTION**

The system is able to restrict or prohibit interfaces that are external from the database. This can be through the use of spoofing, guards, firewalls, etc.

**7.5 SC-13: CRYPTOGRAPHIC PROTECTION**

The system will automatically encrypt any personal (ex: signature, passwords) or classified information to protect the user and database.

**7.6 SC-15: COLLABORATIVE COMPUTING DEVICES**

External media devices are monitored and limited in order to protect the information within the database. This can exclude devices that are able to breach information, such as cameras, microphones, etc.

**7.7 SC-20: SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)**

The system will add additional authentication data to allow remote clients to work from personal computers, but still monitor activity.

1. SYSTEM AND INFORMATION INTEGRITY

## 8.1 Policy and Procedures

System and information integrity is described as the ability to maintain a well-functioning database according to our ideals. The policy reflects any federal laws, executive orders, directives, rules and regulations, and guidance. Responsibilities of the access control include roles, responsibilities, management commitment, coordination, and compliance.

## 8.2 Controls Implemented

**8.3 SI-2: FLAW REMEDIATION**

The system will be able to detect any flaws or bugs within the database and alert the user or authoritative figure to repair those vulnerabilities. This may come in forms such as updates, patches, anti-virus installations, etc.

**8.4 SI-3: MALICIOUS CODE PROTECTION**

The entry and exit points of the system are protected by malicious code protection by the use of firewalls, proxy servers, etc. As malicious code is disguised, the system ensures that the safeguards and consistent scans are implemented.

**8.5 SI-4: INFORMATION SYSTEM MONITORING**

Use of external and internal monitoring protects the database from any attacks. This includes observing events happening at the system boundary, as well as within.

**8.6 SI-5: SECURITY ALERTS, ADVISORIES, AND DIRECTIVES**

If a threat or attack is to occur, the database displays a security message to all users and third-party on the database.