## Media access MP-2

Applicability: All Information systems

Control: The Organization restricts access to organization-defined types of digital media and/ or non-digital media

Supplemental Guidance: Information system media includes both digital and non-digital media. Digital media includes, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, paper and microfilm. Restricting non-digital media access includes, for example, denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers. Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team.

Control Enhancements:

1. Automated restricted access
2. Cryptographic Protection

References:

**NIST Special Publication 800-111**

**FIPS Publication 199**

Priority and Baseline Allocation:

|  |  |  |
| --- | --- | --- |
| **Low** | **Moderate** | **High** |
| MP-2 | MP-2 | MP-2 |

## 

## Plan of Action and Milestones CA-5

Applicability: All Information systems

Control: The Organization Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and

Updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Supplemental Guidance: Plans of action and milestones are key documents in security authorization packages and are subject to federal reporting requirements established by OMB.

Control Enhancements:

1. AUTOMATION SUPPORT FOR ACCURACY / CURRENCY

References:

**OMB Memorandum 02-01**

**NIST Special Publication 800-37**

Priority and Baseline Allocation:

|  |  |  |
| --- | --- | --- |
| **Low** | **Moderate** | **High** |
| CA-5 | CA-5 | CA-5 |

## 

## Information System Backup CP-9

Applicability: All Information systems

Control: The Organization

1. Conducts backups of user-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];
2. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];
3. Conducts backups of information system documentation including security-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];
4. Protects the confidentiality, integrity, and availability of backup information at storage locations.

Supplemental Guidance:System-level information includes, for example, system-state information, operating system and application software, and licenses. User-level information includes any information other than system-level information. Mechanisms employed by organizations to protect the integrity of information system backups include, for example, digital signatures and cryptographic hashes. Protection of system backup information while in transit is beyond the scope of this control. Information system backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information.

Control Enhancements:

1. Testing for reliability and integrity
2. Test restoration using samples
3. Seperate storage using sampling
4. Separate storage for critical information
5. Protection from unauthorized modification
6. Transfer alternate storage site
7. Redundant secondary system
8. Dual authorization

References:

**NIST Special Publication 800-34**

Priority and Baseline Allocation:

|  |  |  |
| --- | --- | --- |
| **Low** | **Moderate** | **High** |
| CP-9 | CP-9(1) | CP-9(1) (2) (3) (5) |

## 

## Incident Monitoring IR-5

Applicability: All Information systems

Control: The Organization tracks and documents information system security incidents.

Supplemental Guidance: Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

Control Enhancements: Automated Tracking / Data collection and analysis.

References: **NIST Special Publication 800-61**

|  |  |  |
| --- | --- | --- |
| **Low** | **Moderate** | **High** |
| IR-5 | IR-5 | IR-5 (1) |

## 

## Incident Reporting IR-6

Applicability: All Information systems

Control: The Organization;

a. Requires personnel to report suspected security incidents to the organizational incident response capability within.

b. Reports security incident information

Supplemental Guidance: The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling.

Control Enhancements:

1. Automated reporting
2. Vulnerabilities Related to Incidents
3. Coordination with supply chain

References:

**http://www.us-cert.gov**

**NIST Special Publication 800-61**

|  |  |  |
| --- | --- | --- |
| **Low** | **Moderate** | **High** |
| IR-6 | IR-6(1) | IR-6 (1) |

## 

## Media Use MP-7

Applicability: All Information systems

Control: The Organization restricts / prohibits the use of defined types of information system media on organization defined information systems or system components.

Supplemental Guidance: Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers). In contrast to MP-2, which restricts user access to media, this control restricts the use of certain types of media on information systems, for example, restricting/prohibiting the use of flash drives or external hard disk drives. Organizations can employ technical and nontechnical safeguards (e.g., policies, procedures, rules of behavior) to restrict the use of information system media. Organizations may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling/removing the ability to insert, read or write to such devices. Organizations may also limit the use of portable storage devices to only approved devices including, for example, devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may restrict the use of portable storage

devices based on the type of device, for example, prohibiting the use of writeable, portable storage devices, and implementing this restriction by disabling or removing the capability to write to such devices.

Control Enhancements:

1. Prohibit use without owner
2. Prohibit the use of sanitization-resistant media

References:

**FIPS Publication 199**

**NIST Special Publication 800-111**

|  |  |  |
| --- | --- | --- |
| **Low** | **Moderate** | **High** |
| MP-7 | MP-7 (1) | MP-7(1) |

## 

## Media Sanitation MP-6

Applicability: All Information systems

Control: The Organization

1. Sanitizes organization defined information system media prior to the disposal, release out of the organization's control, or release reuse by using organization-defined sanitation techniques and procedures with the applicable federal and organizational standards and policies.
2. Brings sanitation mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Supplemental Guidance: This control applies to all information system media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes, for example, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections/words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media containing classified information.

Control Enhancements:

1. Review / approve / track / document / verify
2. Equipment testing
3. Nondestructive techniques
4. Controlled unclassified information
5. Classified information
6. Media destruction
7. Dual authorization
8. Remote purging / wiping of information

References:

**FIPS Publication 199**

**NIST Special Publication 800-66**

**NIST Special Publication 800-88**

**http://www.nsa.gov/ia/mitigation\_guidance/media\_destruction\_guidance/index.shtml**

|  |  |  |
| --- | --- | --- |
| **Low** | **Moderate** | **High** |
| MP-6 | MP-6 | MP-6(1) (2) (3) |

## SC-22 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE

Applicability: All Information systems

Control: The Organization

The Information systems that provide name/address resolution service for an organization are fault tolerant and they implement external and internal separation

Supplemental Guidance: Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers. To eliminate single points of failure and to enhance redundancy, organizations employ at least two authoritative domain name system servers, one configured as the primary server and the other configured as the secondary server. Additionally, organizations typically deploy the servers in two geographically separated network subnetworks (i.e., not located in the same physical facility). For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks including the Internet). Organizations specify clients that can access authoritative DNS servers in particular roles (e.g., by address ranges, explicit lists).

Control Enhancements: none

References:

|  |
| --- |
| **NIST Special Publication 800-81** |

|  |  |  |
| --- | --- | --- |
| **Low** | **Moderate** | **High** |
| SC-22 | SC-22 | SC-22 |

## **SI-12** Information Handling and Retention

Applicability: All Information systems

Control:

The organization handles and retains information in the information system and information output from the system with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Supplemental Guidance:

Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information systems. The National Archives and Records Administration provides guidance on records retention.

Control Enhancements: none

References:

|  |
| --- |
| **NIST Special Publication 800-81** |

|  |  |  |
| --- | --- | --- |
| **Low** | **Moderate** | **High** |
| SI-12 | SI-12 | SI-12 |

## 

RA-1: RISK ASSESSMENT POLICY AND PROCEDURES

* **APPLICABILITY:** Everyone who has access

1. Policy that addresses the implementation of the current risk assessment policy and the steps done to maintain it (procedures). This policy addresses: purpose, scope, roles, responsibility, management commitment, coordination among entities.
2. Regular reviews of current risk assessment policies and procedures.

Risk Assessment Policy and Procedure:

<https://docs.google.com/document/d/18KHRvkmgxsmYPDF3Z6HbjtJzLKrevxCp2jKLCAEs-kA/edit?usp=sharing>

Control Enhancements: NONE

References: NIST Special Publication 800-12, 800-30, 800-100

RA-2: SECURITY CATEGORIZATION

* **APPLICABILITY:** All Information Systems

1. Information and information Systems are in compliance with local and federal laws.
2. Proper documentation of security categories.
3. Assurance that the database administrator has approved of all security categories defined.

<https://docs.google.com/document/d/1JXZhwSQDeowPMJft292fUCZSmLgR_KHmFbXjrBqCCp4/edit?usp=sharing>

Control Enhancements: NONE

References: NIST Special Publication 800-30, 800-39, 800-60

RA-3: RISK ASSESSMENT

* **APPLICABILITY:** All Information Systems

1. Going through a risk assessment for identifying the chance of harm occurring from external or internal entities
2. Documentation of risk assessment results
3. Review results
4. Communicate results to related parties
5. Revisiting risk assessment and making changes as needed that may impact the integrity of the system.

<https://docs.google.com/spreadsheets/d/15TKQbANehGgagyxnlUVKNb7DKxOqr3zHY7huu2aogLU/edit?usp=sharing>

Control Enhancements: NONE

References: NIST Special Publication 800-30, 800-37, 800-60

CA-1 SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES

* **APPLICABILITY:** All Users of Information Systems

Development of documents that detail users roles

1. Creation of policy containing security assessment, scope, purpose and employee interaction with the information system
2. Development of procedures and protocols to follow in events
3. Constant review and update of this policy

Refer to *Security Assessment and Authorization Policy* under **Policy** for the full details.

Control Enhancements: NONE

References: NIST Special Publication 800-12, 800-37, 800-60, 800-53A, 800-100

CA-3 SYSTEM INTERCONNECTIONS

* **APPLICABILITY:** All Information Systems

1. Verification of connections from the information technology systems to other information technology systems.
2. Documentation to keep track of each outbound connection made and accepted
3. Normal review of security requirements

Refer to *Security Assessment and Authorization Policy* under **System Interconnections Security** for the full details.

Control Enhancements: Restriction on External Systems Interconnecting

References: NIST Special Publication 800-199, 800-47

CA-6 SECURITY AUTHORIZATION

* **APPLICABILITY:** System Administrator

1. Assignment of an administrator level for authorization of the database
2. Confidence in administrator authorizing all operations on the information system
3. Normal updates on security authorization.

Refer to *Security Assessment and Authorization Policy* under **Security Authorization** for the full details.

Control Enhancements: None

References: NIST Special Publication 800-137, 800-37

OMB Circular: A-130

OMB Memorandum: 11-33

CA-7 CONTINUOUS MONITORING

* **APPLICABILITY:** All Information Systems

1. Creation of metrics to be monitored
2. Creation of assessments to be monitored and supervised
3. Security control assessments
4. Analysis from security assessments and monitoring
5. Plan of action for responding to analysis
6. Reporting of security status organization

Refer to *Security Assessment and Authorization Policy* under **Continuous Monitoring** for the full details.

Control Enhancements: Trend Analysis & Independent Assessment

References: NIST Special Publication 800-39, 800-37, 800-53A, 800-115, 800-137,

OMB Memorandum 11-33

CA-9 INTERNAL SYSTEM CONNECTIONS

* **APPLICABILITY:** All Information Systems

1. Authorization of connections within the information system to information systems
2. Documentation of all internal systems

Refer to *Security Assessment and Authorization Policy* under **Internal Systems Connections** for the full details.

Control Enhancements: Security Compliance Checks

References: None

PS-4 PERSONNEL TERMINATION

* **APPLICABILITY:** All Information Systems

1. Disabling user access to the system
2. Terminate user’s credentials
3. Having user go through exit interview
4. Retrieving all property owned by the information system
5. Transfer terminated user’s privileges to other user still operating with the organization
6. Notification to system administrator and other users of termination

Refer to the *Personnel Termination Policy* document for full details.

Control Enhancements: Post-Employment Requirements & Automated Notification

References: None

**AC-8 - System Use Notification**

The information system will display a Warning screen, prior to granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:

1. Users are accessing a U.S. Government information system;

2. Information system usage may be monitored, recorded, and subject to audit;

3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties;

4. Use of the information system indicates consent to monitoring and recording;

Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and

For publicly accessible systems:

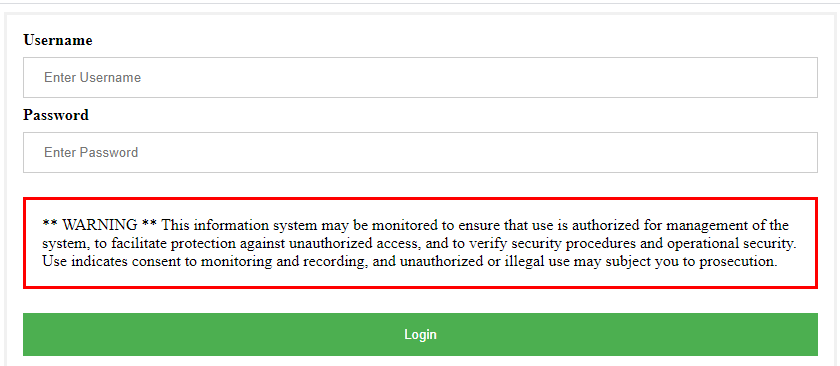
1. Displays system use information [when accessed from information systems logon interfaces with human users], before granting further access;

2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and

3. Includes a description of the authorized uses of the system.

Supplemental Guidance: Control AC-8 applies at all levels of the information system when accessing the database.

Sample login screen with use warning message



**AC-14 - Permitted Actions without Identification or Authentication**

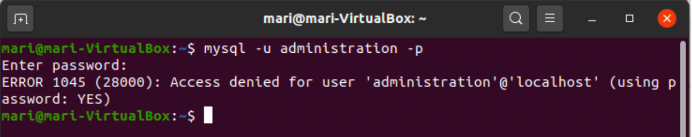
This control addresses instances where no identification and authentication is required. It does not, however, require that such instances exist in a given information system.

In instances where identification and authentication is not required, the information system should ensure to:

1. identify/document specific user actions allowed on the system(s) without identification and authentication,

2. document the supporting rationale for not requiring identification and authentication, and

3. specify any conditions for bypassing identification and authentication mechanisms in order to facilitate operations in emergency situations.



**AT-4 – Security Training Records**

The organization will document and monitor individual information system security training activities for all information system personnel.

Tracking and Reporting Basic and Specialized Training, maintain and report on training compliance by maintaining training records that must include:

1. Name of employee that receives basic and specialized training;

2. Dates and timeframes employee received basic or specialized training;

3. Topics or subject areas covered by specialized training; and

4. Any training completion certifications or successful completion confirmation obtained.

Organization Supervisors are responsible for tracking status of all their reporting employees and review their progress yearly.

All individual Training records should be retained for a period of seven (7) years in accordance with standard retention policy and procedure.

**CM-10 – Software Usage Restrictions**

Control: The organization:

a. Uses software and associated documentation in accordance with contract agreements and copyright laws;

b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Supplemental Guidance: Software license tracking will be accomplished with the use of simple spreadsheets, to record all pertinent software information.

**CP-3 – Contingency Training**

Control: The organization provides contingency training to information system users consistent with assigned roles and responsibilities:

a. Within the organization-defined time period of assuming a contingency role or responsibility;

b. When required by information system changes; and

c. The organization-defined frequency thereafter.

Supplemental Guidance:

Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, regular users may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to set up information systems at alternate processing and storage sites; and managers/senior leaders may receive more specific 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. Training for contingency roles/responsibilities reflects the specific continuity requirements in the contingency plan.

References:

**NIST Special Publication 800-16**

**NIST Special Publication 800-50**

**IA-6 – Authenticator Feedback**

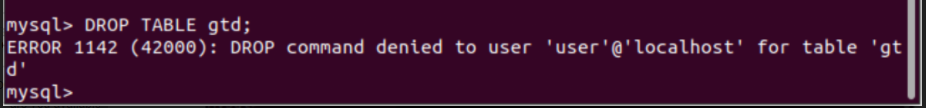
Control:

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Supplemental Guidance:

The feedback from information systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of information systems or system components, for example, desktops/notebooks with relatively large monitors, the threat (often referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with 2-4 inch screens, this threat may be less significant, and may need to be balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly. Obscuring the feedback of authentication information includes, for example, displaying asterisks when users type passwords into input devices, or displaying feedback for a very limited time before fully obscuring it.

Example of user being prevented from removing table



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

Control: The organization:

a. Develops, documents, and disseminates to organization-defined personnel or roles:

1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and

b. Reviews and updates the current:

1. System maintenance policy according to organization-defined frequency; and

2. System maintenance procedures according to organization-defined frequency.

Supplemental Guidance:

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

References:

**NIST Special Publication 800-12**

**NIST Special Publication 800-100**

**PE-8 – Visitor Access Records**

Control:

The organization utilizes an electronic card reader entry system to monitor all access into and out of the building.

The electronic card reader system is used to record all building entrance/exit into daily logs. The organization requires a visitor without an electronic entry card to enter by the main entrance and will be required to check in at the main desk.

1. Any visitor without an electronic card is required to check in at the main desk and provide all required information to the attendant to be added into the system, including the name of person they are to meet (their escort).
2. The attendant will contact the escort and inform them their visitor has arrived and the escort will come to the main desk and accompany the visitor for the duration of their visit.
3. On completion of the visit, the escort will accompany the visitor to the main desk to be checked out prior to leaving the building.

Control Enhancements:

The organization employs automated mechanisms to facilitate the maintenance and review of visitor access records.

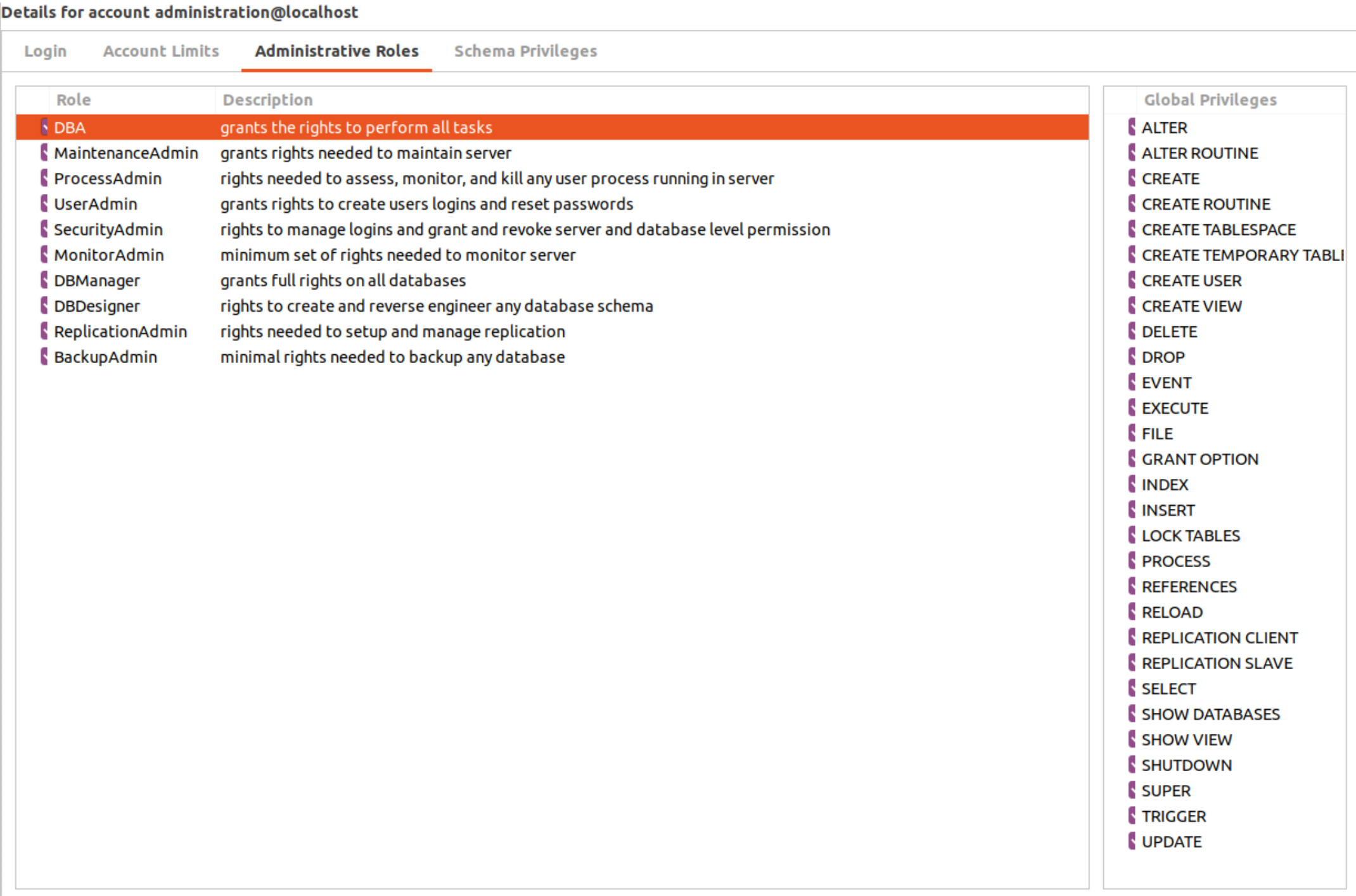
**AC-2 Account Management**

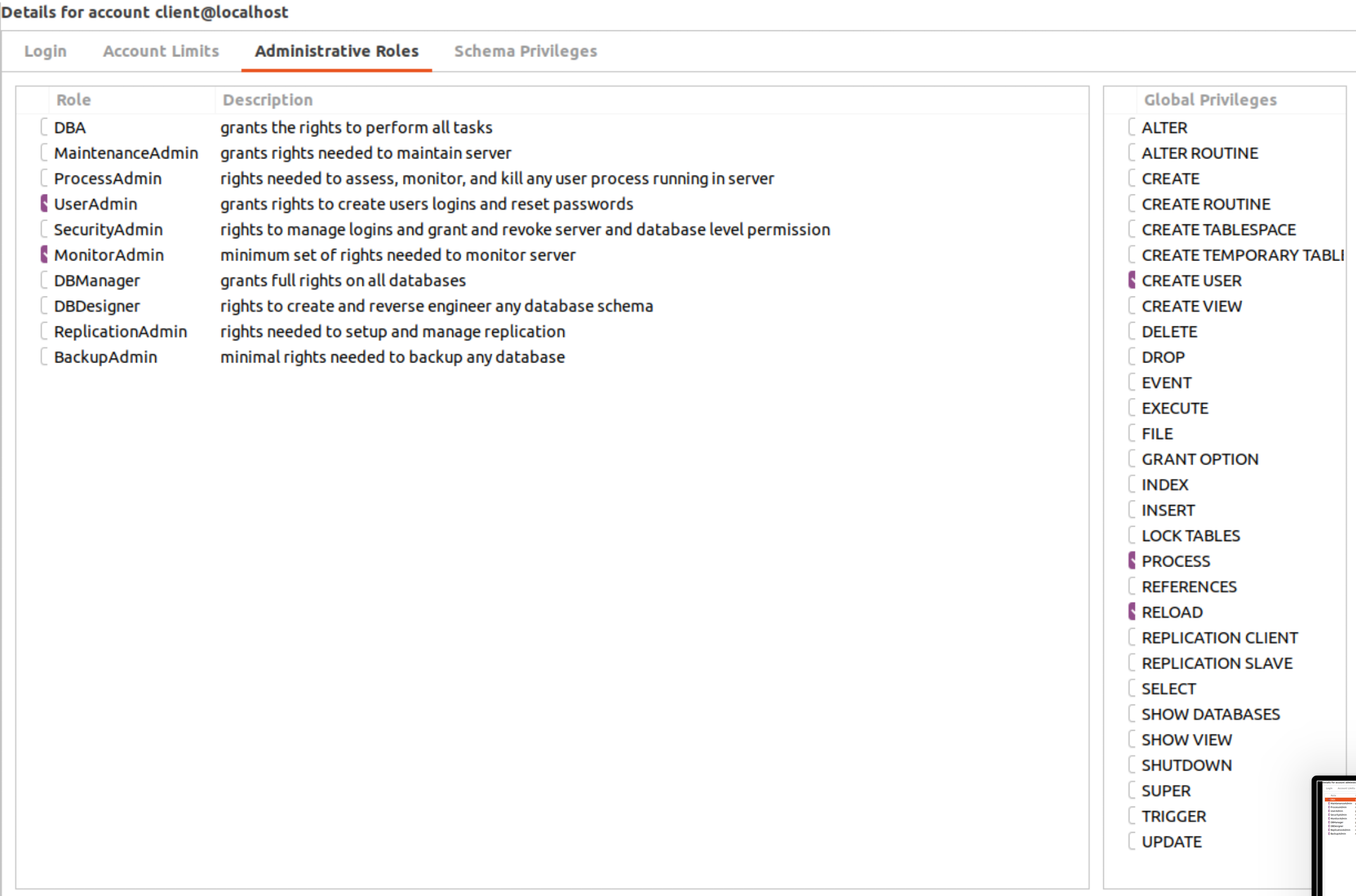
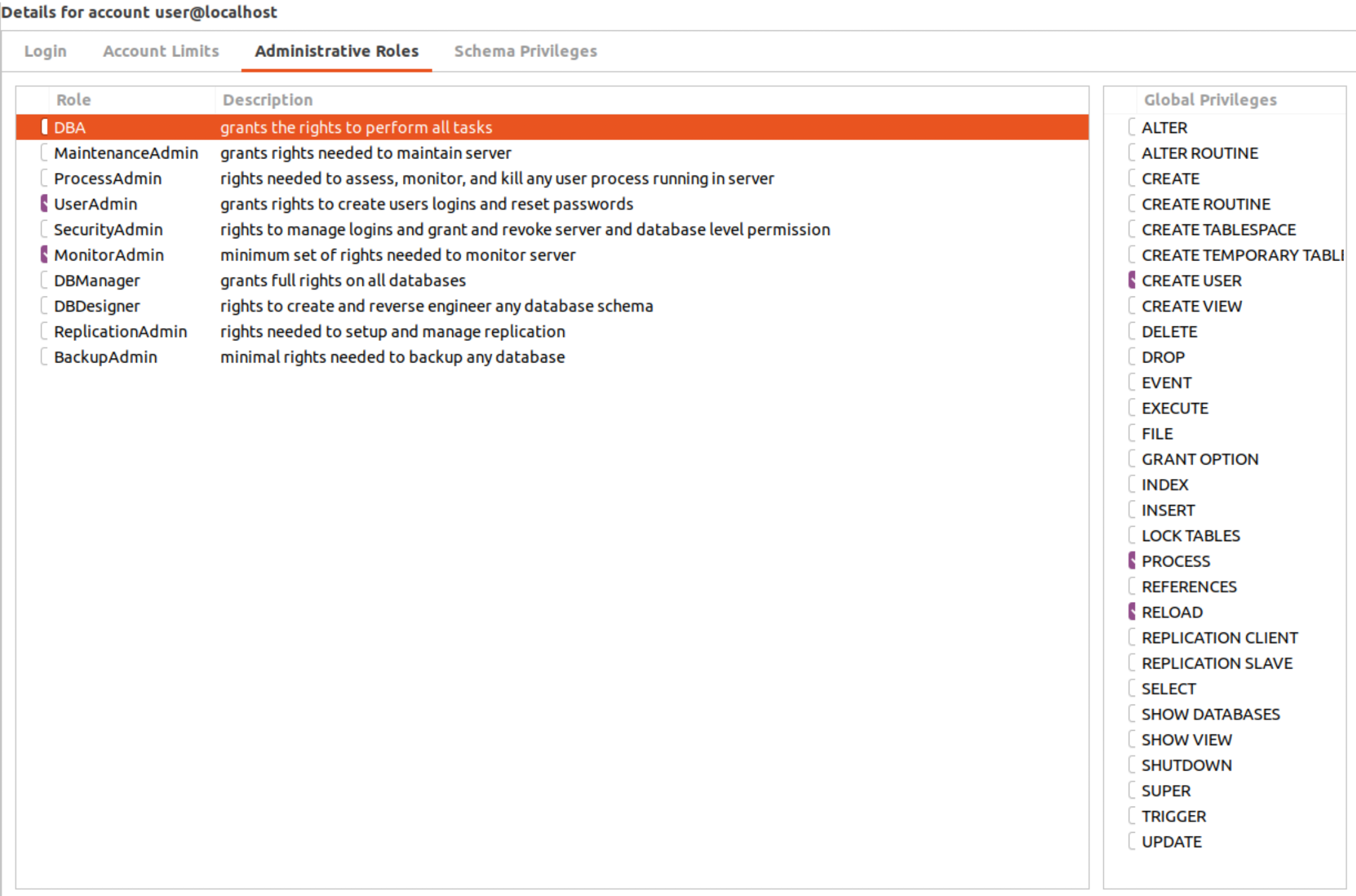
**For all information systems:**

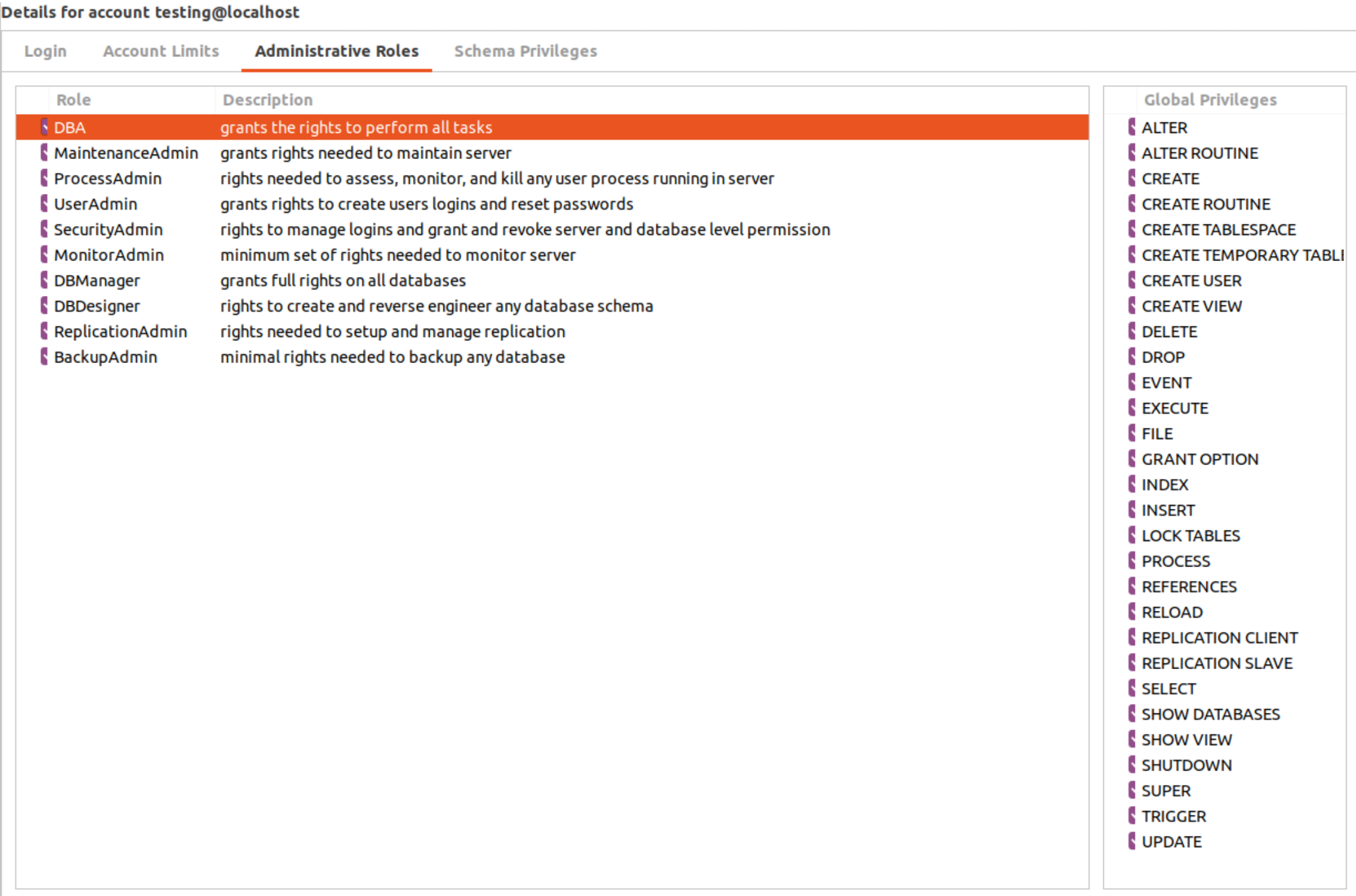
The database administrator (DBA), has created this database (DB) for academic purposes only.

The information found is this database is gathered from the Global Terrorism Database (GTD) made by The National Consortium for the Study of Terrorism and Responses to Terrorism (START) and the Federal Bureau of Investigation (FBI) Annual Hate Crime Statistics publication. There are four roles in relation to this database: DBA, End User, Client, and Testing. The following presents the privileges assigned to each role by the DBA.

Database Administrator System Privileges:



Client Privileges\* CUSTOM End User System Privileges: 

System Testing Privileges: 

**AC-7 Unsuccessful Logon Attempts**

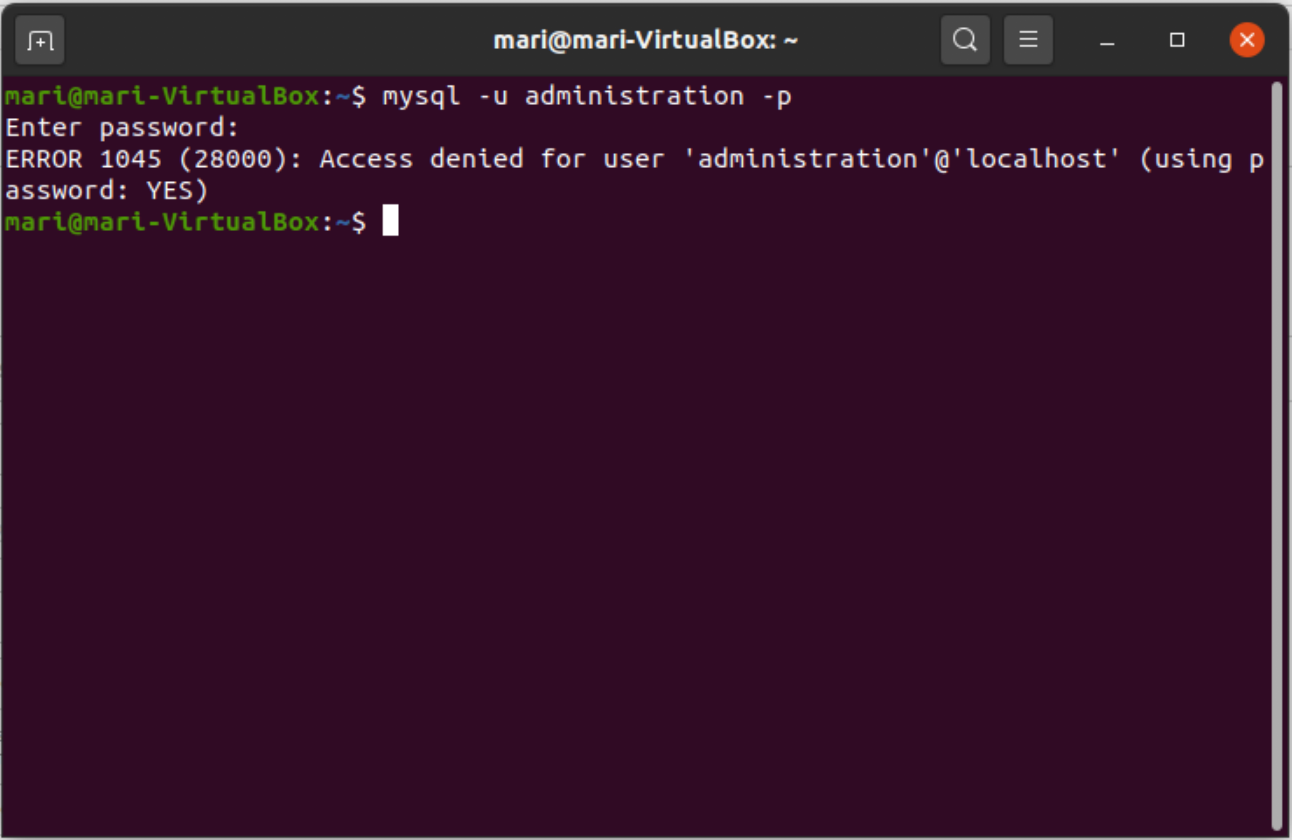
Note: This control applies to all accesses regardless of whether the login occurs via a local or network connection.

**For all information systems:**

1. DBA in coordination with client shall ensure the following:
2. Configure the DB to enforce a maximum of five (5) consecutive invalid login attempts by user during a 15-minute period
3. Configure the DB to automatically lock privileged and non-privileged accounts and delay the next login prompt for 30-minutes when the maximum number of unsuccessful login attempts is exceeded\*.

\*User may contact DBA to release an account prior to the 30 minute lock and to reset password.

References: NIST Federal Desktop Core Configuration (FDCC), United States Government Configuration Baseline (USGCB); Federal Risk and Authorization Management Program (FedRAMP) Cloud Computing Security Requirements Baseline.



**AC-17 Remote Access**

Note: Users of the USCrimes expose information to exploitable vulnerabilities when using teleworking solutions.

**For all information systems:**

The Client must:

a. Establish and document usage restrictions (see PS-3 and PS-6), configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

b.Authorizes remote access to the information system prior to allowing such connections.

Remote access is not permitted without explicit approval. All remote access connections must be authorized prior to allowing such connections.

All remote access will be accomplished through the use of two factor authentication; a username and password or PIN combination.

Data must not be copied from high security systems to a user’s remote machine.Unauthorized users will be disconnected automatically after 24 hours.Users will abide by the above user access guidelines.

**AU-8 Time Stamps**

Note: This control is applied to all tables found in this database. The time stamp generated by the information system includes date and time. The format for this timestamp is Coordinated Universal Time UTC - CST YYYY-MM-DD 00:00:00.000000.

**For all information systems:**

1. DBA in coordination with the client will use the DB internal system clocks to generate timestamps for audit records; and
2. Record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meet the Database Design Requirements set forth by the professor.



**PS-6 Access Agreements**

The purpose of the Access Agreements control is to ensure that users of an information system

have read, understood, and agree to abide by the rules and/or constraints associated with their

access to the information system and its data. These access agreements can include, but are not limited to, documents such as a non-disclosure agreement (NDA), acceptable user agreements, User Policy Agreement, and Rules of Behavior (RoB). Information system users must complete the required access agreement(s) prior to receiving logical access.

**For all information systems:**

1. At the direction of the client, all users must review and abide by the attached User Policy Agreement.

**RA-5 Vulnerability Scanning**

Note: DBA has taken the following action to reduce vulnerability: changed default MySQL port (3306), renamed MySQL username previously ‘root’, enforce unsuccessful logon attempts (see AC-7)

**For all information systems:**

In coordination with the DBA the client will:

a. Scans for vulnerabilities in the DB and hosted applications on a quarterly basis and when new vulnerabilities potentially affecting the system/applications are identified and reported;

b. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:

- Enumerating platforms, software flaws, and improper configurations;

- Formatting and making transparent, checklists and test procedures; and

- Measuring vulnerability impact;

c. Analyzes vulnerability scan reports and results from security control assessments;

d. Remediates legitimate vulnerabilities within thirty days for high-risk vulnerabilities ; within ninety days for moderate risk vulnerabilities in accordance with an organizational assessment of risk; and

e. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

**PS-3 Personal Screening**

Note: The purpose of the Personnel Screening control is to ensure that the client screens and conducts background checks on individuals prior to granting access to the USCrimes DB.

**For all information systems:**

Client must screen individuals prior to authorizing access to the information system and rescreens individuals periodically. Client should refuse user access to information systems until they have:

1) Been granted an interim clearance and the user receives a User ID; and

2) Signed the appropriate access agreements (see PS-6)

The client must require individuals with significant security responsibilities to have completed or in the process of completing a minimum of one (1) course on database concepts with SQL or have an understanding of database management and structure using SQL.

**PE-13 Fire Protection**

**For all information systems:**

The client will employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source. This control is applicable to the USCrimes DB and any additional databases created for the client moving forward..

The client will deploy appropriate fire suppression and detection devices/systems. For example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors. This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

**CA-2 Security Assessment**

**For All Information Systems:**

1) The client, in coordination with the DBA and tester, shall ensure service providers:

1. Assess security controls as early as possible and throughout the system development life cycle process.
2. Provide a security assessment plan prior to conducting assessments.

i) The security assessment plan shall delineate:

(1) The scope of the assessment,

(2) The assessment procedures to be used to determine security control effectiveness,

(a) Assessments shall be conducted in accordance with the latest final version – as determined by the client Senior Agency Information Security Officer (SAISO) – of NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations,

(3) The assessment environment, assessment team, and assessment roles and responsibilities.

ii) The client shall review each system security assessment plan to seek clarification and consensus for security requirements for each specific system under review.

iii) For Client-operated systems, DBA shall review and approve security assessment plans.

iv) For systems operated on behalf of the Client, FBI, GDT and DBA shall review and approve security assessment plans.

1. Follow the security assessment plan and notify approvers of any changes to the plan necessary to complete the assessment once the assessment begins.

## 

## 

## 

## 