REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF FINANCE
BUREAU OF INTERNAL REVENUE

July 10, 2020

REVENUE MEMORANDUM ORDER NO. 28-2020

SUBJECT **UPDATED POLICIES AND PROCEDURES FOR THE GRANTING AND REVOCATION OF SYSTEM ACCESS**

TO **ALL INTERNAL REVENUE OFFICIALS, EMPLOYEES AND OTHERS CONCERNED**

---

1. OBJECTIVE

The existing procedures on the granting and revocation of system access are hereby updated to strengthen the security control, protect the confidentiality of information asset, and streamline access processing.

This also aims to harmonize previously issued policies and procedures, as follows:

- Unnumbered Memo dated July 6, 2020 - Revised Acceptable Use Policy (AUP)
- Unnumbered Memo dated April 2, 2019 - Information Security Awareness Briefing for BIR Service Providers and On-The-Job Trainees
- Unnumbered Memo dated November 6, 2017 - Conduct of Information Security Awareness Briefing for BIR Newly-Hired Employees
- RMO No. 53-2018 – Revised BIR Form No. 0044 (Request for System Access/Access Revocation)
- RMO No. 17-2019 – Amendment to RMO 33-2001 in the Granting of Regular Access to Users of the BIR-Integrated Tax System (ITS)

2. DEFINITION OF TERMS

- **Acceptable Use Policy** refers to the acknowledgement of users and third parties that they understand and accept their responsibilities when accessing BIR's information and/or information systems and agree to comply with the BIR policy.
- **Account Registry** refers to a centralized manual registry of each system with the list of individual users, the user ID and the specific access rights defined.
- **Account Revocation** refers to the cancellation/deletion/suspension of user account due to any of the following: retirement, resignation, leave of absence, transfer of assignment, dormant account and so on.
- **Account Request Summary Report** refers to the list of BIR personnel/contractors whose request for system access was received and processed on a given day.
- **Database Administrator** refers to a person responsible for the creation, maintenance, backups, querying, tuning, user rights assignment and security of the system's databases.
- **Deactivated Account** refers to a user account that was disabled due to dormancy or non-usage
- **Dormant Account** refers to a user account that has been inactive for at least three (3) months.
- **Information Assets** refers to any data, information or material generated, gathered, compiled, stored or utilized by BIR in the course of its operations, regardless of format or form (either electronic or physical document).
- **Justification for Special Access** refers to a memo issued by the Head of Office / Project Manager indicating reason/s for use/need of access by user/requestor
- **Non-Disclosure Agreement** refers to a contract by which one or more parties agree not to disclose confidential information that they have shared with each other as a necessary part of doing business together.
- **Process Owner** refers to an office/individual that has approved management responsibility on system/business process with respect to control over the development, production,

BUREAU OF INTERNAL REVENUE
RECEIVED
AUG 17 2020
9:15 am
RECORDS MGT. DIVISION

maintenance, use and security of assets.

- **Project Manager** refers to a BIR official who is in-charge of the planning and execution of a particular BIR project.
- **Role Definition Request Form** refers to the form to be used in requesting for creation/ modification/deletion of role
- **Regular Access** refers to user access granted based on the:
  - Approved Security Access Matrix (SAM) and with the required appropriate trainings;
  - Approved SAM and role definition/job performance for at least a year (for users with deficiencies or without the required/appropriate training)
- **Security and Access Matrix** refers to a centralized registry of each system with the list of user designation/functions and their corresponding access rights as approved by the Process Owner.
- **Special/Temporary Access** refers to user access granted based on:
  - Designation/function defined in SAM but without the required appropriate trainings, or role definition/job performance is less than a year;
  - Designation/function is not in the access privileges defined in SAM
- **System User** refers to individuals granted with explicit authorization to access, modify, delete and/or utilize information based on the SAM.
- **System Administrator** refers to a person responsible for the maintenance of user account, upkeep, configuration, and reliable operation of computer systems and servers.
- **Third Parties** refer to partners, government agencies, contractors, temporary employees, consultants, third party service providers, taxpayers, on-the job trainees and the public.
- **User ID** refers to a unique symbol or character string used by a system to identify a specific user. It may also refer to username, user account, login name, or login account.

3. POLICIES

3.1. Request for User Account Creation/Extension/Revocation/Reactivation

3.1.1. Users shall accomplish the appropriate Access Request form depending on the type of request:

3.1.1.1. Request for System Access/Access Revocation – BIR Form No. 0044 (see Annex A)

3.1.1.2. eFPS Access Request Form – BIR Form No. 0043 (see Annex B)

3.1.2. Appropriate documents shall be attached to Access Request form:

3.1.2.1. BIR Employees

3.1.2.1.1. Acceptable Use Policy (AUP) - BIR personnel requesting access for the first time shall accomplish the AUP, which shall cover all the requester's succeeding access requests within the year and shall be renewed annually

3.1.2.1.2. Copy of required certificate of training/s (Information Security Awareness Briefing and/or Systems Training)

3.1.2.1.3. Justification/endorsement from the Head of Office, if necessary Report for Duty for BIR personnel, if necessary

3.1.2.2. BIR Service Providers (contractors/job orders)

3.1.2.2.1. Acceptable Use Policy (AUP) - BIR Service Providers requesting access for the first time shall accomplish the AUP, which shall cover all the requester's succeeding access requests within the year and shall be renewed annually

3.1.2.2.2. Copy of required certificate of training/s (Information Security Awareness Briefing and/or Systems Training)

3.1.2.2.3. Justification/endorsement from the Head of Office, if necessary Report for Duty for BIR personnel, if necessary

3.1.2.2.4. Non-Disclosure Agreement (NDA)

BUREAU OF INTERNAL REVENUE
RECEIVED
AUG 17 2020
9:15 am
RECORDS MGT. DIVISION

3.1.2.2.5. Copy of signed contract

3.1.3. Attendance to Information Security Awareness Briefing is pre-requisite before system access be granted to newly-hired employees and BIR Service Providers.

3.1.4. BIR Service Providers shall be given access only upon submission of approved NDA and signed contract. They shall only be granted special/temporary access with justification from the Head of Office/Project Manager.

3.1.5. BIR officials and employees who are subject of regular movement, whether by reason of promotion, reassignment, leave of absence for thirty (30) days or more, resignation or transfer/secondment to other government agencies, instrumentalities/office within BIR, shall request for revocation of access.

3.1.6. The Head of Office/Project Manager shall be responsible for requesting revocation of access of personnel under his/her jurisdiction, in case:
- 3.1.6.1. Employee failed to report to their new place of assignment within the prescribed period per issued Revenue Travel Assignment Order (RTAO)
- 3.1.6.2. Employee who are considered Absent without Leave (AWOL) for thirty (30) days or when there are grounds for recommending the dropping from the revenue service
- 3.1.6.3. Third parties whose contract/engagement with the BIR has ended

3.1.7. Accomplished/Signed Access Request form and attachment shall be submitted to:
- 3.1.7.1. Security Management Division – Contractors / National Office Users except Large Taxpayers Service
- 3.1.7.2. Concerned Data Center – Regional Users including Large Taxpayers Service

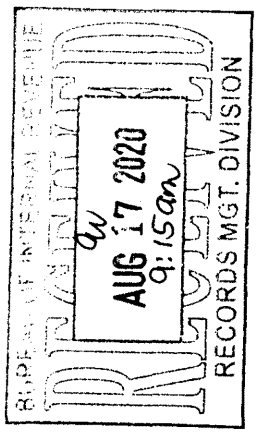
3.1.8. Personnel Adjudication Division (PAD) shall furnish Security Management Division (SMD) copy of the approved order of suspension/dismissal from the Office of the Commissioner (OCIR), Ombudsman, Civil Service Commission (CSC) or any judicial or quasi-judicial administrative body within three (3) days from receipt of the approved order, for processing of revocation/suspension of account privileges.

3.2. **Evaluation and approval of all access requests shall be guided by the following:**

3.2.1. All access requests with incomplete information shall not be processed.

3.2.2. The level of access (regular or special) to be granted to BIR personnel shall depend on the designation/function role defined in the approved SAM of BIR system/s, required/appropriate trainings, and role designation/ job performance

3.2.3. Request for special access shall be justified or endorsed by the Head of Office/ Project Manager. It shall be for a specified/limited duration and shall be revoked automatically after the lapse of the specified/limited duration.



3.2.4. Users who were given special access due to lack of required training can be given a regular access if they performed the actual role at least one year and shall be justified by the Head of Office.

3.2.5. A request for access shall not be processed/granted if the user has any existing system access account from his/her previous place of assignment, unless a corresponding approved revocation of access form is submitted together with the current request for access form.

3.2.6. All access requests received by Revenue Data Center (RDC)/Security Management Division on or before 10:00 AM shall be processed and endorsed to System

Administrator (SysAd) and/or Database Administrator (DBA) on or before 12:00 noon of the same day. Access requests received beyond 10:00 AM shall be processed and endorsed to SysAd and/or DBA on or before 12:00 noon of the following day.

3.2.7. Endorse access request forms to:
- 3.2.7.1. SysAd – for user access request;
- 3.2.7.2. DBA – for technical user access request to operating system level and/or database level

3.2.8. All access requests received by SysAd and/or DBA on or before 12:00 noon shall be processed within two (2) days.

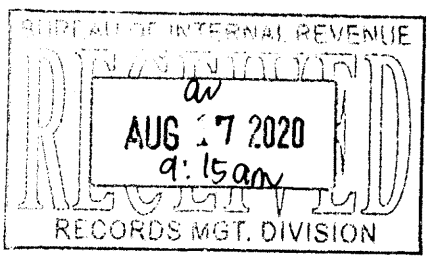
4. PROCEDURES

4.1. Request for User Account Creation/Extension/Revocation/Reactivation

4.1.1. The Requester/User shall
- 4.1.1.1. Accomplish the appropriate access request
- 4.1.1.2. Forward the duly accomplished form with the appropriate supporting document/s to the Head of Office/Project Manager for approval;
- 4.1.1.3. If request was approved/granted, receive thru email:
  - 4.1.1.3.1. notification that the request for access was processed
  - 4.1.1.3.2. temporary password and instruction to change password upon log-on;
- 4.1.1.4. Otherwise, receive notification that the request for access was not approved and the reason for disapproval

4.1.2. The Head of Office/Project Manager shall
- 4.1.2.1. Evaluate and sign the request form;
- 4.1.2.2. Endorse the request form and supporting document/s to the SMD or respective RDC;

4.1.3. The SMD/RDC Receiving/Processing Officer shall
- 4.1.3.1. Receive the request forms and supporting documents from the Head of Office/Project Manager; and review/evaluate the request with regard to:
  - 4.1.3.1.1. Document completeness and accuracy of information - in case of incomplete information or supporting documents, coordinate with the concerned user/requester to comply within five (5) days from notice, otherwise the request form/s shall not be processed;
  - 4.1.3.1.2. Job designation/Role in accordance with Security Access Matrix;
  - 4.1.3.1.3. Trainings attended



- 4.1.3.2. If the request is compliant:
  - 4.1.3.2.1. Process the request and endorse the request to SMD Chief/ RDC Head for approval
  - 4.1.3.2.2. Prepare the Access Request Summary (ARS) report; and endorse ARS report together with the access request forms to SysAd and/or DBA
  - 4.1.3.2.3. Update the Account Registry upon receipt of ARS report from the SysAd and/or DBA

- 4.1.3.3. If the request is not within the approved SAM:
  - 4.1.3.3.1. Endorse the access request to the concerned Process Owner for approval

4.1.3.3.2. Receive approved/disapproved access request from the concerned Process Owner

4.1.3.3.2.1. If the access request is approved, process the access request following the procedure mentioned in item 4.1.3.2

4.1.3.3.2.2. Otherwise, inform the user thru email that the access request was not approved and the reason for disapproval

4.1.4. The SMD Chief/RDC Head shall

4.1.4.1.1. Approve/disapprove the request form

4.1.4.1.2. Sign the ARS report

4.1.5. The SysAd shall

4.1.5.1. Receive the ARS report and approved request form/s.

4.1.5.2. Create/reactivate/revoke access and sign-off request form/s. Revocation of all access request shall be done within twenty-four (24) hours upon receipt;

4.1.5.3. Notify the requester thru email that the request for access was processed;

4.1.5.4. Release log-in and password to the user/requester thru email;

4.1.5.5. Update ARS report and submit to SMD/RDC thru email.

4.1.6. The DBA shall

4.1.6.1. Receive ARS report and approved request form/s;

4.1.6.2. Grant/update/revoke database access privilege and sign-off request form/s. Revocation of all database access request shall be done within twenty-four (24) hours upon receipt;

4.1.6.3. Notify the requester thru email that the request for access was processed

4.1.6.4. Release log-in and password to the user/requester thru email;

4.1.6.5. Update ARS report and submit to SMD/RDC thru email.

4.1.7. The SMD shall:

4.1.7.1. Receive copy of the approved order of suspension/dismissal from the Office of the Commissioner (OCIR), Ombudsman, Civil Service Commission (CSC) or any judicial or quasi-judicial administrative body for processing of revocation/suspension of account privileges;

4.1.7.2. Prepare request for revocation/suspension of account privileges and ARS report; and endorse to SysAd and/or DBA

4.1.7.3. Update the Account Registry upon receipt of ARS from SysAd and/or DBA

4.1.7.4. Inform the originating office that the access of the personnel concerned has been requested for revocation/suspension.

4.2. **Request for Password Reset/Unlocking of Account**

4.2.1. The User shall

4.2.1.1. Notify their respective Requester to log request in the Service Desk System the request for access re-set/ account unlocking;

4.2.1.2. Receive temporary password/notification the account has been unlocked thru email;

4.2.1.3. Access the system/application and change the password.

4.2.2. The Requester shall:

4.2.2.1. Log request in the Service Desk System for ticketing;

BUREAU OF INTERNAL REVENUE
RECEIVED
AUG 17 2020
9:15am
RECORDS MGT. DIVISION

If the BIR Service Desk System is inaccessible and/or the Requester is not available, the User can directly raise the request thru email to the concerned SMD/RDC personnel. The process for request for User Account Creation/Extension/Revocation/Reactivation shall be followed.

4.2.2.2. Close ticket/issue resolved by SysAd/DBA

4.2.3. The Service Desk of respective SMD/RDC shall
4.2.3.1. Assign the ticket to the SysAd and/or DBA.

4.2.4. The SysAd and/or DBA shall
4.2.4.1. Reset the password/unlock the account
4.2.4.2. Notify the user through email:
4.2.4.2.1. temporary password and instruction to change password upon log-on; and/or
4.2.4.2.2. account has been unlocked and that user can proceed with the transaction
4.2.4.3. Update status and provide action taken in the Service Desk System.

4.3. **Request for Creation/Modification/Deletion of Role**
4.3.1. The SMD shall:
4.3.1.1. Receive new/revised SAM from Process Owner
4.3.1.2. Accomplish the Role Definition Request Form to request for creation/ modification/deletion of role based on the new/revise SAM
4.3.1.3. Endorse accomplish form to DBA for implementation
4.3.1.4. Receive the signed-off request form from DBA

4.3.2. The DBA shall:
4.3.2.1. Receive the Role Definition Request Form from SMD
4.3.2.2. Create/modify/delete role and sign-off request form
4.3.2.3. Endorse the signed-off request form to SMD

4.4. **Periodic Review and Maintenance of User Accounts**
4.4.1. The SMD shall:
4.4.1.1. Perform Access Inventory and Review on user accounts and their access rights granted on a weekly basis
4.4.1.1.1. Identify the sample population from the system generated user access granted, to be included in the review;
4.4.1.1.2. Check each sample based on the test attributes indicated below:
4.4.1.1.2.1. The user is an active employee;
4.4.1.1.2.2. The request is supported with properly endorsed and approved request form;
4.4.1.1.2.3. The user's access rights are appropriate in accordance with the SAM.

4.4.1.2. Perform Access Review of revoked user accounts on a monthly basis;
4.4.1.2.1. Check the System Generated User Access List to determine whether the user accounts of the sample employees who resigned/terminated/transferred have been timely and completely revoked;
For systems that are not equipped with the facility to generate user access list, SMD shall use the Account Registry;

4.4.1.3. Conduct Inactive Accounts Review to ensure that user accounts that remain inactive for over ninety (90) days shall be disabled immediately. This is to prevent retention of unnecessary or unauthorized rights

4.4.1.4. Update of Security and Access Matrix (USAM):
4.4.1.4.1. Review the list of special access granted and check if there is a need to update the current SAM.

BUREAU OF INTERNAL REVENUE
RECEIVED
AUG 17 2020
9:15 am
RECORDS MGT. DIVISION

4.4.1.4.2. Prepare the USAM request form (BIR Form 0036) and endorse to Process Owner and DCIR-ISG for approval.
4.4.1.4.3. Revise the existing SAM and endorse the revised/updated SAM together with the approved USAM request form to Process Owner for approval.
4.4.1.4.4. Receive the signed updated SAM
4.4.1.4.5. Provide RDCs, SysAd and DBA with copy of the signed updated SAM.

4.4.1.5. Communicate with the Process Owner and SysAd/DBA any exceptions noted from the review

4.4.2. The SysAd/DBA shall perform User Account Maintenance
4.4.2.1. Upon receipt of memorandum based on the results of the review conducted by SMD and/or approved SAM from SMD:
4.4.2.1.1. Revoke/suspend the user accounts or modify the access rights
4.4.2.1.2. Create/modify/deletion of role, if system requires
4.4.2.2. Notify SMD of action taken

5. REPEALING CLAUSE

All other issuances and/or portions thereof inconsistent herewith are hereby revoked and/or amended accordingly.

6. EFFECTIVITY

This Order shall take effect immediately.

CAESAR R. DULAY
Commissioner of Internal Revenue

036335

