Account Management NON USE Policy

The purpose of this document is to outline the Identity and Access Management Policy of user accounts that have not been used in a specific timeframe.

Account Management team will run a monthly audit of User accounts, the team will determine whether a user has not logged in/changed their passwords in 90 days/logged into TLE in 120 days.

Once this is determined the user account will be disabled with notes stating – ACCOUNT DISABLED PER NON USE – mm/dd/yyyy (date the account was disabled). List of all accounts that have been disabled will be sent to LSA Distribution Group asking for REVOKE CSR for military, FLMA, other admin reasons or a TERMINATE CSR for employees no longer with the agency.

If a user attempts to log back in, the user will need to call the Service Desk; the Service Desk will state the user will need to contact the LSA to have an Update CSR submitted to enable the account.

After two months of the user account being disabled, Account Management will again send out notification to LSAs. List of all accounts that have been disabled will be sent to LSA Distribution Group asking for REVOKE CSR for military, FLMA, other admin reasons or a TERMINATE CSR for employees no longer with the agency.

When user returns to work after being disabled, LSA to complete UPDATE CSR to enable the account.

Account Management NON USE Policy

The purpose of this document is to outline the Identity and Access Management Policy of user accounts that have not been used in a specific timeframe.

Account Management team will run a monthly audit of User accounts, the team will determine whether a user has not logged in/changed their passwords in 90 days/logged into TLE in 120 days.

Once this is determined the user account will be disabled with notes stating – ACCOUNT DISABLED PER NON USE – mm/dd/yyyy (date the account was disabled). List of all accounts that have been disabled will be sent to LSA Distribution Group asking for REVOKE CSR for military, FLMA, other admin reasons or a TERMINATE CSR for employees no longer with the agency.

If a user attempts to log back in, the user will need to call the Service Desk; the Service Desk will state the user will need to contact the LSA to have an Update CSR submitted to enable the account.

After two months of the user account being disabled, Account Management will again send out notification to LSAs. List of all accounts that have been disabled will be sent to LSA Distribution Group asking for REVOKE CSR for military, FLMA, other admin reasons or a TERMINATE CSR for employees no longer with the agency.

When user returns to work after being disabled, LSA to complete UPDATE CSR to enable the account.

Identity and Access Management

Purpose

Internal Account Management process on how to handle the calls/tickets for a Cyber Security Incident.

Process

In the matter of a security risk with a user's domain account, Cyber Security will contact the OIC stating that action needs to be taken on a specific users account.

The OIC will generate a quick ticket (Cyber Disable Request); they will change the password on the user's account, create the ticket, assign the ticket to Account Management and contact Account Management on call immediately.

Account Management will do the following to the user's account within about an hour time:

Move the account to Account Disabled OU

In the Description field add the following verbage –

ACCOUNT DISABLED PER CYBER INCIDENT #### - <<DATE>>

Disable the users account

If you are not able to help with the disabling of the account let the OIC person know so they can contact another team member.

Once the account has been disabled note this in the ticket and leave the incident open until word from Cyber to enable the account.

When Cyber contacts Account Management to enable the account.

Account Management will do the following:

Move the user back to the appropriate OU

Take out the ACCOUNT DISABLED message

Enable the users account

Reset the user's password

Email the password to the Cyber Tech that called to enable the account

DPS Executive Management Process

When a User is either promoted or making a lateral move as an Director, Deputy Director, Assistant Director (AD), Deputy Assistant Director (DAD), Chief, Assistant Chief, and Regional Commander the following items are automatically given/retained:

- Remote Access, remains or given if does not already have.
- Active Sync – work order to be sent to Mobile team to change budget code if needed.
- Internet privileges – carry with them if applicable; do not grant if they do not have.
- DPS_Everyone sending ability

Identity and Access Management

Purpose

Policy for requesting access to a user's home directory, email account or items on computer.

What is needed

In order to gain access to a user's home directory, email account, and/or computer data there are a few items needed:

1) CSR filled out
    a. Terminate if the user has left the agency and you are needing access
    b. Revoke if the user is suspended or the account needs to be only disabled not terminated
2) Business Justification sent to the email box Data-Security from the DAD
3) Time frame for needing the access to the email account if monitoring incoming email

Information

Home directory access: this is the folder on a file server that only the user can access while at DPS. If needing access to the users home directory after the person has left the agency or account is disabled a CSR is needed, on the CSR it will ask who the home directory will move to. Once approval has been received the home directory will be placed in the designated user's home directory.

Email Access: Once approval has been received and a CSR is submitted, a work order will be created for a tech to come out and create a PST file for the designated user to have and attach to their email

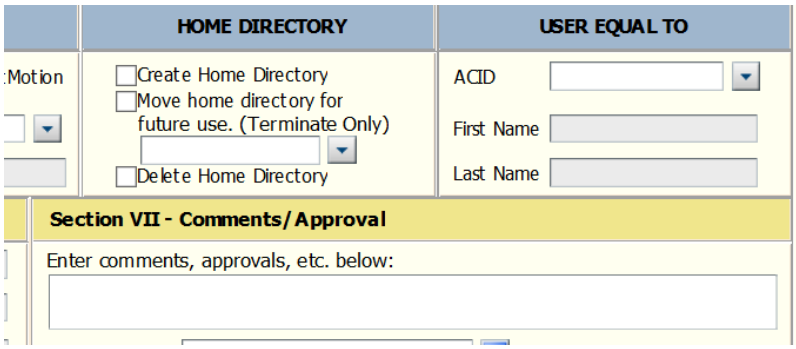
Incoming Email Access: Once all approvals have been received and CSR submitted and a time frame is stated the SMTP address will be added to the designated users account. At the end of the time frame the SMTP address will be removed from the designated account.

Computer data: Approval from DAD and business justification will be needed, once all has been received a work order will be created for the tech to come out and get the data needed to the designated user.

LSA Roles:

Submit the Terminate/Revoke CSR:

There is a section on the CSR (Home Directory), in this section if home directory move is needed, select the Move Home Directory for future use (Terminate Only), also put in the drop down box the designated user that will receive the data. In Section VII – Comments/Approval, please put in this area if email access or computer data is needed.



The LSA will also need to make sure that the request for access goes to the DAD of the Division with business justifcation and possible time frame. Once this has been received send the approval to Data-Security mailbox.

DAD Role:

Approve the business justification for moving or access the user's data.

Account Management Role:

To ensure all approvals, have been received with business justification and time frame received if needed, after all has been received grant the access

NOTE:

If Account Management does not receive proper approval for this request in 10 business days the account will be terminated without access granted. An email to the LSA will be sent from the team member that has the CSR stating the deadline, which will be the final warning.

For Investigation purposes Cyber Security could need access to user's home directory, emails and/or computer data. In order to grant Cyber access, an approval from the CISO will need to be provided.

ICT Analyst Unrestricted Internet Access

Account Management has received the approval from Cyber Security and DAD Avant to allow any new ICT Analyst to have unrestricted internet access due to their job duties.

When Account Management receives a NTFS or CSR to add the user to the group because the user is an Analyst for ICT add the user to the following group:

Grp_internet_users_unrestricted_ICTAanlyst

When a user is no longer an ICT Analyst and transfers from that position, Account Management will remove the group from the user account.

Texas Department of Public Safety
Rules of Behavior for Remote Access

This document outlines the conditions the Texas Department of Public Safety (TXDPS) requires for the use of remote access. By signing this agreement, the user agrees to abide by the TXDPS Rules of Behavior and Cyber Security Policies (ref. DPS General Manual, Chapter 26, *Information Management Service)* for the use of remote access. It is the user's responsibility to ensure they understand and follow the established policies for the protection, storage, and handling of all TXDPS Data. This includes Personally Identifiable Information (PII), Criminal Justice/Intelligence (CJIS), Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry (PCI) data. In addition, the following rules apply to the use of remote access.

The user understands and agrees to the following:

Requirement 1: Audit

There is no expectation of privacy for any data processed, stored, or transmitted while remotely connected to the TXDPS network. TXDPS can access and audit all data or equipment at any time without any notice to the user.

Requirement 2: State Equipment

The user will only use TXDPS issued equipment to connect to the network. All computers connected to the TXDPS network will be scanned for current updates and virus patches. Access will be denied and sessions terminated if appropriate patch levels are not maintained on the equipment.

Requirement 3: Security Profiles

The equipment issued by TXDPS for remote access is configured with security profiles to ensure the protection of the equipment being issued. The user will not attempt to remove, disable, or bypass any security settings enabled by TXDPS.

If any tampering of the equipment's security profile is attempted or it is discovered that the user made unauthorized modifications, TXDPS will immediately deny access to the network and recall the equipment.

Requirement 4: Media Protection Requirements

The user must ensure that the remote location has adequate physical security to protect against any unauthorized personnel viewing or gaining access to TXDPS information or information systems.

The user is fully responsible for the protection of the equipment and any media (i.e. printed material, CDs, DVDs, etc…) in their possession. The user will ensure they follow

appropriate destruction and handling requirements for the information they have access to in accordance with department policy.

Requirement 8: Awareness and Training

The user will complete training as required, and there will be an annual validation of remote users to evaluate if remote access is still required. Users that fail to submit their revalidation by the required suspense date will have their remote access privileges revoked.

User Acknowledgement and Acceptance

The user understands and agrees they are accountable for their actions when using remote access and that they may be held liable in administrative, civil, or criminal proceedings for any unauthorized actions found to be intentional, malicious, or negligent.

I certify by my signature below that I have read and fully understand this document and agree to comply with its contents.

_____	_____	_____
Printed Name of User	Signature of User	Date

I certify that I understand my responsibility for implementing these policies and ensuring the user is aware of their responsibilities while using remote access.

_____	_____	_____
Printed Name of Manager	Signature of Manager	Date

Process for granting/removing elevated domain privileges

Account Management requires the following to grant a user elevated domain privileges:

1) CSR stating which rights need to be granted
2) Manager approval with business justification

Once rights are no longer needed we will need the following:

1) CSR stating to remove the rights granted
2) Manager approval, stating when to remove the rights.

Texas Rangers Unrestricted Internet Access

Account Management has received the approval from Cyber Security and DAD Malinak to allow any new Texas Ranger (commissioned) to have unrestricted internet access do to their job duties.

When Account Management receives a Transfer CSR for a new Texas Ranger add the user to the following group:

Grp_internet_users_unrestricted_rangers

TLE Domain Account Credential (ACID) Reassignment

Purpose

The purpose of this policy is to deny reassignment of user ACID after leaving DPS and returning to DPS employment.

User Termination Process

When a user leaves DPS, a LSA must submit a termination CSR for the Account Management Team to delete the account from Active Directory and any other applicable programs. If there are rights to a program outside of the Account Management Team, a work order is submitted by Account Management to the appropriate group to remove the rights.

User Addition Process

Users returning to DPS after previously working for the agency, ACID assignment must follow the same process as new employees and receive a new ACID based on sequential numbering system. The Account Management Team will deny any request to reassign a previously used ACID.

Reason for Denial:

Employee ACID accesses are assigned based on the last position the employee held within the agency. If returning to the agency in a different position, using a previously used ACID would result in the employee having the same accesses as when they left the agency resulting in the employee having access to records they should not have in their new role.