**State of Georgia Privileged Access Document of Understanding, Deviation Acceptance Letter and Request Form**

**Version 2.0**

**Last Updated: Dec/04/2019**

**Location: GETS Home > SMM-Enterprise Documents > IT Service Management Procedures > Access Mgmt > Ancillary Documents**

**1. Introduction**

This deviation acceptance letter specifically relates to the customer's use of privileged access as it applies to theiraccount.

UNISYS Global Server Systems Operations – State of Georgia best practices restrict Administrative or Root level authority to only UNISYS designated personnel for security and control measures. This document is presented in response to the customer’s request for shared Administrative or Root level access to the environment. Once privileged access has been granted to personnel outside of UNISYS it is impossible to have as secure an environment as it was prior to the privileged access request. Every effort will be made to understand the customer's need for privileged access and UNISYS will work with the customer to provide an alternate means of accomplishing the activity without compromising security where possible.

**2. Privileged Access Use, RCA and Defect Ownership**

Shared possession of privileged access mandates shared responsibilities between UNISYS and the customer for support and change control in the environment. Consequences from the use of privileged level user IDs may result in adverse impact to the environment. As a precaution, UNISYS and the customer will collaborate closely to coordinate privileged access to the servers. The customer will inform UNISYS of any changes made under Administrator or Root on the servers.

UNISYS and customerpersonnel will collaborate on Root Cause Analysis (RCA) of outages when privileged access is shared. UNISYS Client Relations Representatives will attend any Executive Review meetings and are responsible to accurately and completely represent the customer's participation in events resulting in an RCA. UNISYS and customer personnel will collaborate on Audit Data Findings when privileged access is shared. If an audit finding is determined to be customer owned, the customer agrees to ownership of the audit defect.

The following is GTA / Unisys requirements:

GTA will:

A.1 Authorize and approve the creation, deletion or modification of user IDs and passwords for SOG personnel for the systems software under UNISYS management

A.1.1 Conduct a Quarterly Employment Verification (QEV) on SOG user ids; UNISYS will provide the ID listing via a one-way communication only and UNISYS will make corrections as directed by SOG.

A.1.2 Conduct an annual Continued Business Need (CBN) Verification on SOG userids; UNISYS will provide the ID listing via a one-way communication only and UNISYS will make corrections as directed by SOG.

A.1.3. Conduct an annual Privilege Revalidation for the SOG user IDs; UNISYS will provide the ID listing via a one-way communication and UNISYS will make corrections as directed by SOG.

**3. Prohibited Activities for Customer Privileged (Administrator / Root) Access Use**

Customer use of privileged user IDs must adhere to the following restrictions:

* Submit different technologies into separate request forms. (i.e. Unix, Windows, Database, etc)
* Will not reboot, restart or power off systems.
* Will not grant elevated privilege to alternate user IDs.
* Will not uninstall security patches or back level system components and/or tools installed to preserve the integrity and security posture of the server and/or environment.
* Will not make use of a customer server to explore and collect information regarding the UNISYS network environment including tools/admin network layers.
* Will not administer user IDs (will not modify current permissions nor create user IDs, etc.) or make modification to the active directory/ldap ACL schema unless specifically described in the privileged access request and reviewed/approved by the UNISYS Account Team and SA/Middleware teams in advance of the change.
* No functions are to be performed that are not defined and documented in this Privileged Access Request Form in advance. See Appendix A.
* Will not install additional software or upgrades without license ownership.
* For Windows systems, the customer will make no changes to Operating System parameters without UNISYS participation and prior approval. The customer will not:
	+ Create a new user
	+ Modify user account settings such as Password Never Expires
	+ Modify permissions of system files and directories
	+ Modify startup and shutdown scripts or the startup value of any services
	+ Change file system attributes
	+ Place files in the system file structure (%systemroot%)
* For UNIX systems, sudo su - is prohibited. Specific sudo commands must be listed in Appendix A.
* For UNIX systems, the customer will make no changes to Operating System parameters without UNISYS participation and prior approval. The customer will not:
* Change system file attributes and path
* Modify operating system files
* Add or alter a user ID, password or group
* Override the PASSWD or NOPASSWD tag
* Use the log\_file option to redirect the syslog
* Modify startup or shutdown scripts
* Place any files within the operating system file structure
* Change system file attributes and paths

Any exceptions to prohibited activities must be explicitly noted in Appendix A, “Work to be Performed”.

As the requester, I confirm that at least one of the following is true for each command requested and that I am responsible for the accuracy of these statements and/or compliance to their requirements; and will accept any audit finding should I be inaccurate:

* The command(s) **does not** contain the ability to escape to a shell as root
* The command(s) **does** contain the ability to escape to a shell as root and maintains individual accountability to each command executed in a root shell for audit purposes; and I will denote which command(s) permit such shell escapes.
* The command(s) **does** contain the ability to escape to a shell as root and fails to maintain individual accountability to each subsequently issued commands. Any access to the command will be accompanied by a problem, incident, or change record. I will denote which command(s) permit such shell escapes.

**4. UNISYS Recourse, ID Revocation, and Undocumented IDs**

UNISYS reserves the right to immediately revoke access of any customer user ID which performs tasks not listed in Appendix A. If abuse of privileged access is determined, revocation of the offending user ID will occur immediately followed by notification to the ID Owner or Customer Representative and UNISYS Client Relations. The offending user ID will then be reviewed for reinstatement or deletion.

In the event a privileged user ID does not have supporting documentation, including all Approvals required in Appendix A, the user ID is subject to immediate deletion.

1. **Signatures of UNISYS Client Relations and Global Services Systems Operations - State of Georgia**

The signatures on the request form below, representing UNISYS and the customer are in agreement on all content in this document and are committing their respective organizations to the specified responsibilities as documented. This deviation acceptance form will be in effect from the requested start date through the end date which must be specified and is not to exceed 90 days. Privileged access will be revoked within three business days of the end date. A new or revised deviation acceptance form will need to be approved by the expiration date or privileged access will be revoked.

Note: IDs that are created with a set authorization time period are to be validated every 365 days for privledged access users or access will be disabled. Accounts should be reviewed every 90 days for validation of short term access requests. New PRIV ACCESS REQUEST’s should be submitted to maintain access beyond specificed time or 365 days.

Note: **There is a 10 business day turn-a-round in which the Priv Access Request Review Team has to review and sign form. If onboarding a new employee, then add “On-Boarding” in request and in email header.**

1. **Privileged Access Request Procedure**
2. Requester completes each section of Appendix A. Errors and incomplete forms will be rejected and cause delays in the fulfillment of your request. If privileges are required for the installation of new SW or changes to the environment, the PRIV ACCESS REQUEST must include a CRQ.
	* Save and rename with the following naming convention:
		+ GTA Customer Privileged Request Form – V2.0 - Agency XXXX Requester XXXXX.doc
	* Once the form is complete, submit form to UNISYS PRIV ACCESS REQUEST Review at SOGPrivilegeAccess@Unisys.com.
3. The UNISYS Privileged Access Review Board will review requests to determine complexity, requirements and validity.
4. Post PRIV ACCESS REQUEST Board review, one of the following will occur:
	* Approved PRIV ACCESS REQUESTs - UNISYS Security sends Approved PRIV ACCESS Requests to GTA Security for sign-off. GTA Security approves the PRIV ACCESS REQUEST and sends the completed PRIV ACCESS REQUEST to the requester/originator of the email request. All approved privileges are temporary. Any changes to the requirements of an approved will require a new PRIV ACCESS REQUEST to be submitted to the PRIV ACCESS REQUEST Board.
	* Rejected PRIV ACCESS REQUESTs – The UNISYS PRIV ACCESS REQUEST Board sends rejection feedback to the requester/originator of the email and the supporting ARM. Once corrections are complete, the Requester re-submits the corrected PRIV ACCESS REQUEST to the UNISYS PRIV ACCESS REQUEST Board
5. Once the requester receives approval, the requester creates a User Account Activation request. The agency enters this request via the GETS Products and Services Catalog along with the signed PRIV ACCESS REQUEST attached. Request content must always map to PRIV ACCESS REQUEST content e.g. PRIV ACCESS REQUEST supports the request. If the Service request Number contains an altered PRIV ACCESS REQUEST from the approved PRIV ACCESS REQUEST file the Service request Number will be rejected.
	* After approval in the GETS Products and Services Catalog, a Service request Number is created and UNISYS will grant the access within the agreed upon service target for this request type.
	* Once the Service request Number is complete, the requester will receive a confirmation via email.

Note - Contact your Agency Relationship Manager if assistance completing the Privileged Access Form is needed.

**Appendix A**

**Privileged Access Approval Form for UNISYS Global Server Systems Operations – State of Georgia Customers**

**Complete each section of the Appendix in full or the form will be rejected. If the form below is incomplete or contains errors this will cause a delay in the implementation of your request. Save the file as GTA Customer Privileged Request Form – V2.0 - Agency XXXX Requester XXXXX.doc. Submit completed forms to UNISYS PRIV ACCESS REQUEST Review at SOGPrivilegeAccess@Unisys.com.**

**Section A - Role**

**Agency Name:**

**Account Code:**

**Requester’s Department Name:**

**Requester’s Job Role / Function:**

**Section B - Justification**

**Business Justification for Privileged Access:** (Provide specific detail)

**Change Request Number:**

**Section C - Purpose**

**Software to be Supported:** (Provide specific detail)

**Section D - Tasks**

**Work to be Performed:** (Provide specific detail)

**Section E (UNIX) – Activities**

|  |  |  |  |
| --- | --- | --- | --- |
| **User ID or Unix group** | **Hostname** | **Specific command or Unix groups (leave blank for SSH access only)** | **Service Account ID Owner (new or transfer), if applicable** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

*Provide specific commands using* ***full command path****, relative path is not allowed.*

*“sudosu –“ or root access is against security policy and will not be allowed.*

*If Unix group is to be provided privileges, include all current members in section F.*

*Unix groups cannot be added to Unix groups.*

**Section E (Active Directory) – Activities**

|  |
| --- |
| **Reset passwords / Unlock accounts** |
| User ID or Group: | Domain:Agency: |
| **Create workstation computer accounts &****Join workstations to domain** |
| User ID or Group: | Domain:Agency: |
| **Update general user information** |
| User ID or Group: | Domain:Agency: |
| **Create group** |
| User ID or Group: | Domain:Agency: |
| **Update general group information** |
| User ID or Group: | Domain:Agency: |
| **Other. Describe in detail what access is required, for whom,** **to which containers/objects, and against which object types:** |
|  |
| *If security group is to be provided privileges, include all current members in section F.* |

**Section E (Intel) – Activities**

|  |  |  |  |
| --- | --- | --- | --- |
| **User ID or group** | **Hostname** | **Remote Desktop/Administrator/Other** | **Service Account ID Owner (new or transfer), if applicable** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| *If group is to be provided privileges, include all current group members in section F.**If provided group is an AD group, prefix its name with “domain\” ex: “SOG\GroupName”.**If requesting ‘other’ activities, provide specific local group, permissions, or privileges required.* |

**Section E (Mainframe) – Activities**

|  |  |  |
| --- | --- | --- |
| **User ID** | **Hostname** | **Privileges** |
|  |  |  |
|  |  |  |
|  |  |  |

**Section F–Duration 365 Days Max (Per requirement, all accounts require annual review)**

**Start Date (mm/dd/yyyy):**

**End Date (mm/dd/yyyy):**

**Is this a renewal or revalidation of existing privilege? (Yes/No):**

If Yes, no action will be taken with the User ID listed above; this form is required for audit purpose only.

**Section G – Approvals**

**You have two options for approvals:**

1. Print this document, obtain approver physical signatures, and scan the signed document. Attach it to the service request.
2. Obtain approvals via email. Save the email approvals as a PDF file and attach it to the service request.

By approving this document, you are stating you authorize the User ID(s) listed above to have privileged access for the specified duration and agree to all of the items listed in this document.

 **Date:**

**X Email Address:**

**Requester**

 **Date:**

**X Email Address:**

**Agency CIO/ISO Representative**

 **Date:**

**X Email Address:**

**GTA Security Representative**

 **Date:**

**X Email Address:**

**UNISYS Security Representative**