admin

THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION

Privileged Account Activation / Change Request
Enterprise Systems
IT-3000C
(Rev. 6/2017)

Instructions: This form should be used only for requesting, renewing, terminating or updating a privileged network (SCPRIVID) account. Information must be provided for all required fields (as indicated by *).   Submit completed form to the Department of Administration Service Desk at servicedesk@admin.sc.gov.

General Information		
Agency / Division *		Date *
Requested Action ☐ New ☐ Renewal ☐ Termination ☐ Role Update	Effective Date	Termination Date

User Information			
Name*	Office Phone*	Mobile Number (Work)*[1]	SCNETID*
Email*			

[1]Mobile number is required for two-factor authentication

Privileged Roles

☐ Enterprise   ☐ Domain   ☐ Identity *(SCNETID)*   ☐ Identity *(SCPRIVID)*   ☐ Email   ☐ Desktop Support

☐ Group Policy   ☐ Group   ☐ Service   ☐ System *(Please specify)* _____

☐ Other *(Please specify)* _____

Justification for Request / Additional Information

Acknowledgement

I assume full responsibility for protecting the security of the privileged account and the confidentiality of information I encounter in the use of the account. I understand that my assigned privileged account is for my use only in performance of job duties and that it must not be shared or used by other individuals. I understand that I am responsible for all activity and transactions that occur under my account and I will immediately notify Department of Administration Service Desk of any suspect activity in my account. I understand that I am responsible for keeping privileged use passwords secure and confidential and recognize that privileged passwords must be different from my standard account password. I will not attempt to use my assigned privileged level access to circumvent enterprise security systems. I understand that my privileged account must not be used for daily use activities and must not be used for accessing resources located on the Internet. I understand my privileged account will be actively monitored and an audit trail of activities will be created and reviewed by the Division of Information Security. I understand that any violation of account policy, security policy, agency policy or law will result in the immediate termination of privileged account access and authorization. In addition, appropriate disciplinary action may be taken in accordance with State and Agency disciplinary policies and progressive disciplinary process.

Privileged Access will be disabled once one of the following occurs; (1) the time frame for requested privileged access expires, (2) the job tasks have been completed for which the privileged account was created, or (3) one year has passed since the request for privileged access was submitted and approved.

By signing below, I acknowledge the responsibility and fully understand and accept the risk and responsibility associated with privileged level access.

Assigned User: _____   _____   _____
                               Signature   *Print Name*   *Date*

Manager / Supervisor: _____   _____   _____
                               Signature   *Print Name*   *Date*

Deputy CISO / Designee: _____   _____   _____
                               Signature   *Print Name*   *Date*

Deputy CIO / Designee: _____   _____   _____
                               Signature   *Print Name*   *Date*

Data Classification: Internal Use