

The Division of Technology Operations manages infrastructure and services supporting business functions for the Department of Administration and its customers. Some technical operations and administrative functions may require elevated rights in order to perform specific tasks and job duties.

Instructions: Complete all required fields (as indicated by (*)). Submit completed form to the Department of Administration's Service Desk at servicedesk@admin.sc.gov. Incomplete or unclear forms may cause delay in completing request.

General Information* (Complete for all requests)			
Agency / Division *			Date *
Account	Department	Effective Date	Expiration Date
Action <input type="checkbox"/> New Account <input type="checkbox"/> Renewal <input type="checkbox"/> Termination <input type="checkbox"/> Role Change			

User Information			
Name*	Phone*	Email*	SCNETID*

Privileged Roles (Select necessary privileged roles)				
<input type="checkbox"/> Enterprise Admin	<input type="checkbox"/> Domain Admin	<input type="checkbox"/> Identity Admin	<input type="checkbox"/> Policy Admin	<input type="checkbox"/> Email Admin
<input type="checkbox"/> Identity Admin (PRIV)	<input type="checkbox"/> Group Admin	<input type="checkbox"/> Service Admin	<input type="checkbox"/> System Admin	<input type="checkbox"/> Other (Provide below)

Additional Instructions

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 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 Information Security of any suspect activity not associated with my activities. 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 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: _____
Print Name
Signature
Date

Deputy CISO / Liason: _____
Print Name
Signature
Date

Deputy CIO / Director: _____
Print Name
Signature
Date