COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF HUMAN SERVICES

INFORMATION TECHNOLOGY POLICY

Name Of Policy: **TACACS Accounts**	Number: **POL-ENSS003**
Domain: **Network**	Category: **TACACS Account Approval Process**
Date Issued: **01/24/12**	Issued By Direction Of:
Date Revised: **03/07/2016**	Clifton Van Scyoc, Chief Technology Officer

Abstract:

How to obtain a Cisco Terminal Access Control Access Control System (TACACS) username and password?

General:

In order to gain access to any of the DHS, Aging or Insurance Cisco Routers, Switches, Riverbed devices or Wildpackets Sniffers, a TACACS username and password are required.

Policy:

All requests for a TACACS username and password in order to access network equipment will be sent by email to the DHS Unit Chief for the Network and Telecommunications Unit. If approved the unit chief will forward the accounts unto Verizon to physically create the accounts.

A master list of the TACACS accounts, the date created and revoked will be kept by the unit chief on a server data share. This master list will be reviewed quarterly for any accounts whose access is no longer needed.

All TACACS password must meet the following requirements:

Contain 3 of the following 4 criteria: Upper Case, Lower Case, Numbers and Special Characters

Be at least 8 digits long.

Passwords will expire every 45 days.

Exemptions from this Policy:

There will be no exemptions to this standard.

Refresh Schedule:

All policies and referenced documentation identified in this standard will be subject to review and possible revision annually or upon request by the DHS Information Technology Standards Team.

Policy Revision Log:

Change Date	Version	Change Description	Author and Organization
1/24/12	1.0	Policy Written	Matthew Messinger, BIS-DTE
10/9/13	1.0	Reviewed no changes necessary	Matthew Messinger, BIS-DTE
3/13/15	1.0	Reviewed; changed DPW to DHS agency	Robert Gordon, BIS-DTE
3/07/2016	1.1	Updated the CTO's name	Aamir Qureshi, BIS-DTE