# PAS Administrator Professional Requirements

Best Practices

# Documentation Information

| | |
|---|---|
| Document No. | CAUSPS0003 |
| Document Type | Best Practices |
| Classification | CyberArk Restricted |
| Intended Audience | CyberArk Employees and PIM Customers |
| Author | Dmitriy Sokolovskiy, Director of Implementation Services |
| Date Authored | May 8, 2012 |
| Last Updated | August 13, 2015 |
| Abstract | This document describes the minimum professional requirements for the PAS Administrator position |

## Revision History

| Revision Number | Author | Revision Summary |
|---|---|---|
| 201205-01 | D. Sokolovskiy | First Draft |
| 201205-02 | D. Sokolovskiy | Second Draft |
| 201208-01 | D. Sokolovskiy | Third Draft |
| 201508-01 | D. Sokolovskiy | Final Draft |

## Definitions

This document describes the Standard Operating Procedure in preparation for the deployment of the Enterprise Password Vault solution. Deviations from the baseline must be justified and documented for each customer.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

# Description

Following are minimum required and minimum desired professional experience for the role of a PAS Administrator in charge of deploying and maintaining a CyberArk PAS solution:

# Required Experience and Skills

- A background in Information security systems with specific knowledge around Access Control.
- Hands on Windows 2008 and 2012 Server Administration experience – 2+ years
- Hands on IIS administration experience – 1+ years
- Hands on Active Directory and LDAP queries experience – 1+ years
- Functional understanding of TCP/IP networks and Firewalls
- Functional understanding of following protocols: TCP, UDP, DNS, NetBIOS, HTTP, HTTPS, SMTP, SNMP, SSH, SSL
- Functional understanding of database concepts
- Prior experience as technical lead for enterprise software deployments

# Desired Experience and Skills

- Windows GPO management experience
- Basic UNIX system administration
- Basic database administration
- Basic scripting experience
- Experience with the following technologies/products: Identity Management, SIEM, Authentication and SSO, System Monitoring and Alerting, Ticketing Systems, MSCS and Web Load Balancing solutions.
- Conflicts between GPO elements introduced with the Domain membership with internal components of the Digital Vault. Such conflicts will require non-standard troubleshooting techniques which will impact CyberArk Support SLAs and increase the RTO.