1.12 - Privileged Account Standard

Introduction

Privileged accounts are used to access and maintain various computer systems on the West Virginia University at Parkersburg network. A privileged account is an account that has elevated administrative rights. A user with a privileged account has the ability to access confidential information, change data, and destroy data. Privileged accounts can pose a security risk to the college if proper controls and procedures are not in place.

Policy

Access Control Measures

- Access to critical systems, networks, files, data and processes is limited based on the principle of least privilege and need to know according to job responsibilities. Access will be granted to the least amount of data and privileges needed to perform a job.
- Access rights will be confirmed for a user to ensure that he or she only has the access necessary to perform job responsibilities.
- A procedure is established for employees to request privileged account access.
    - This request must be approved by a higher-level administrator.
- A unique login will be created for each person that has been granted privileged access. It is imperative that privileged account access information is never shared.
- Privileged accounts must have strong passwords (at least twelve characters with numbers and symbols) and must be changed every six months.
- Compliance requirements of federal regulations (FERPA, SOX, GLBA, etc.) and industry standards (PCI, DSS, etc.) pertaining to privileged accounts will be followed.
- OIT will investigate and report incidents that violate protective measures or cause unacceptable risk to privileged accounts.
- OIT will track and document the issuance and usage of privileged accounts.

Violations

Violation or non-compliance of this standard may lead to disciplinary action up to and including termination.