Server Build Standards, Documentation, Business Continuity Planning, and Password Management

New River Community and Technical College has established the following procedures for server build standards, documentation, business continuity planning, and password management:

1) **Server Build Standards**
    a. **Password Policy**: New River uses Exchange 2010 and the Active Directory as the primary authentication for most of our hosted services. Strong passwords (meeting complexity requirements) were implemented on July 9, 2012. The maximum password age is 178 days and the minimum password length is 6 characters (a number, a lowercase and an uppercase letter, and a special character are required).
    b. **Account lockout policy**: The account lockout duration is 10 minutes and the account lockout threshold is 5 invalid attempts.
    c. **Audit policy**: Not currently defined in the Active Directory, but instead, we rely on the audit log created in IssueTrak, our Help Desk trouble-ticket system. This allows us centralized access to the information and access is limited to users in technology services who need the information.
    d. **Share access**: Shares are only created upon request for the individuals included in the request.
    e. **Application installation**: Employees are able to install applications on their own computers, but most often they request that technology services perform these installs. Lab computers are locked with Deep Freeze to prevent any new installations by users and technology services staff members unlock them to perform installs as needed.
    f. **Event log settings**: Not defined, but on local workstations the maximum log file size is 20480KB with standard install of Windows 7 and if necessary events will be overwritten.
    g. **Security options**: Local administrator is enabled. Guest account is disabled. Interactive login is enabled. Do not display last username is enabled. Requires domain controller authentication is enabled to logon. Smart card is disabled. Force logoff is disabled.
    h. **User Rights Assignment**: Administrators and domain admins can add workstations to the domain. Allow logon through Remote Desktop Services is enabled, but restricted through the firewall by blocking ports so that only admins using VPN access may remotely access a workstation from outside the New River network.
2) **Documentation**
    a. **System Monitoring Procedures**

i. Event logs are available on all workstations and servers to monitor as necessary.
ii. WSUS (used with Secunia) and Microsoft Endpoint Protection are tools used to monitor necessary updates and patches.
iii. Alerts are enabled to monitor the facilities servers in VMware Vsphere 5.x.
iv. Server Administrator uses Remote Network Watcher to monitor systems.
v. Alpha Technologies monitors core network devices (routers, switches, gateway, firewalls, etc.) for any downtime with alerts emailed to New River staff as necessary.

b. System Maintenance and Change Control

i. WSUS (and Secunia) provide updates for all servers and computers. System Administrator has these scheduled for 2am on Thursday. Routine monitoring ensures that all computers receive updates as needed.
ii. Servers providing mission essential services are scheduled for updates during non-business hours.

c. Access Rights Administration

i. Users are assigned only the rights needed to perform required functions.
ii. HR informs IT of all new employees and accounts are created accordingly. In the event an employee leaves or is terminated, HR informs IT and the user's account is disabled. This includes access to Banner and other systems as appropriate.
iii. AD accounts are checked periodically for last logon activity and disabled as needed.
iv. Access rights are updated based on personnel or system changes.
v. Periodic reviews ensure that access rights have been appropriately assigned.
vi. Security classes are used in Banner to provide role-based access.

3) Backup/Recovery and Business Continuity Planning

a. With about half of all New River services delivered from the Cloud, our internal business continuity planning only pertains to services hosted at New River.
b. The primary data center is located in room O-15 on the Raleigh County Campus. Physical access to the room is controlled with numeric keypad on

door and locks on each of the two racks/cages. Password-level authentication provides a third level of security.

c. All virtual machines are backed up via Windows Server Backup and SMVI on a daily basis. Windows server backup backs up to a Dell MD1000, while the SMVI agent creates a snapshot of the machine on the NetApp storage datastors.
d. A Tangent Datacove backs up all emails on an internal hard drive.
e. The System Administrator handles the routine replacement of failed hard drives and other data center equipment. Redundant RAID arrays allow him to perform this without interruption of services.
f. In the event that all data center equipment on the Raleigh County Campus is destroyed, only limited data from the RCC data center would be preserved. We are currently migrating our entire data center to Charleston so that Alpha Technologies will host our primary data center and we will host the secondary. This is hoped to be helpful as we plan our move of the RCC to Beaver at the end of this calendar year.

4) **Password Controls**

a. See item #1 for Active Directory authentication and password issues.
b. Authentication for Banner: INB requires 1-30 alphanumeric characters (it does not accept special characters). SSB requires 6-15 alphanumeric characters. Dated password expiration is not currently enforced for Banner. Primary access to these systems is through the College portal, which uses the AD for authentication.