I. PURPOSE

The purpose of this standard is to establish a baseline for configuring computer servers within the University.

Units may implement more restrictive controls and safeguards than those outlined herein; however, units implementing less restrictive controls and safeguards shall receive approval from the University Chief Information Security Officer (CISO) before the server is implemented in production.

Exception requests shall be submitted to/through the UKAT Service Desk. The UKAT Service Desk will then assign and forward requests to the University CISO for disposition. If desired, dispositions can be appealed to the University Chief Information Officer (CIO).

Units implementing cyber security safeguards, policies and practices that are not explicitly addressed by this standard shall reference and implement the SANS Critical Security Controls and/or the National Institute of Standards and Technology (NIST) cyber security policies, procedures, standards and guidelines (i.e., http://csrc.nist.gov/publications/PubsTC.html, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.)

II. APPLICABILITY

This policy is applicable to all personnel who acquire, configure, implement or maintain computer servers that collect, store, process or transmit University information/digital assets.

III. THE STANDARD

1. General

   a. Virtualized servers should be used whenever possible (as opposed to using physical servers.) There are numerous benefits to using virtualized servers such as lower cost, better management and ease of use. This standard addresses the safeguarding and configuring of both hardware and virtual servers.

   b. Units implementing server cyber security safeguards, policies, practices, standards, configuration settings, security controls that are not explicitly addressed herein shall reference and implement the SANS Critical Security Controls and/or the National Institute of Standards and Technology (NIST) cyber security policies, procedures, standards and guidelines (i.e., http://csrc.nist.gov/publications/PubsTC.html, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.)

   c. All system administrators shall comply with UKAT’s Data Classification Standard.

2. Versioning

   a. The most recent stable version of the operating system that is supported by the vendor shall be installed.

   b. The server shall have the most current service packs and patches installed.
c. All exceptions shall be documented.

d. All patch and change management procedures shall be documented with each Unit’s standard operating procedures or information security program.

e. All installed updates and patches should be tested on or in a development environment according to each Unit’s standard operating procedures before the server is placed into production.

3. Accounts

   a. All accounts that are not needed shall be removed (not merely disabled.)

   b. Any and all default passwords shall be changed and shall comply with the UK Password Policy. This also applies to all service or daemon accounts.

   c. Personal LinkBlue accounts shall not be used for service accounts.

   d. Service accounts shall not have mailboxes attached to or associated with them.

   e. All accounts (service or local) shall comply with the UK Password Policy.

   f. If Active Directory is required or used in any capacity, a Domain Administrator account on the local server should be used (for additional management benefits.)

   g. Assignment of Privileges

      1) Administrators shall adhere to the principle of least privileges for all user accounts. The principle of least privileges is that accounts shall be given only the amount of rights, privileges and access needed to perform the necessary task(s) or to perform his/her job (i.e., be given the least amount of rights and privileges needed to accomplish the work.)

      2) The creation of accounts, the deletion of accounts and all changes to an account’s rights, privileges and access shall be documented.

4. Physical and Environmental Safeguards

   a. All servers shall be in physically-secure locations with adequate power and cooling resources.

   b. Only authorized persons shall have physical access to where the server is located.

   c. Physical ingress and egress should be monitored. Best practice is to document all ingress and egress to/from where the server is located.

5. Media Access

   a. If any media access contains data that is classified as either confidential or sensitive, technical safeguards (or compensating controls) shall be implemented and documented. Media access is defined to be any removable form of data storage such as a USB drive, an external hard drive, a writeable CD/DVD.
6. **File System and Data Access (authorization)**

   a. Servers shall be configured to ensure that only authorized users can access files or software on the server. This is generally accomplished by either authenticating the user at the local server level or by extending trust from another server that has performed the authentication. System administrators who opt to permit another server to perform the authentication are still responsible for ensuring that only authorized users access the local server.

   b. File shares that provide access to user populations across organizational unit boundaries or to “any” account, shall be regularly monitored and audited for unwanted changes.

   c. Accounts and users that no longer need rights or access to a file share shall have that access or rights removed.

   d. All vendor, third party and service accounts shall be removed/deleted as soon as they are no longer needed.

   e. All user accounts shall be periodically assessed and those no longer requiring access shall be removed/deleted. This audit/process shall be performed, at a minimum, annually. Proof of audit shall be retained for one year.

   f. All servers shall be on UK’s private IP address space and not publicly-accessible.

7. **Services**

   a. All services shall be disabled by default.

   b. All services that are enabled shall be documented (as to why and when they were enabled.)

   c. All default or factory-set passwords shall be changed (and shall comply with the UK Password Policy.)

   d. All vendor, third party and service accounts and any default or factory-set accounts remaining on the server shall be justified and documented prior to being put into production and, if applicable, prior to being made publicly-accessible.

   e. All vendor, third party and service account passwords shall comply with the UK Password Policy.

   f. All vendor, third party and service accounts shall be removed/deleted as soon as they are no longer needed.

   g. Server out-of-band management IP addresses shall not be publicly accessible (e.g., DRAC interface. This does not include protocols or apps like SSH or RDP, although we highly recommend all IP addresses be private unless needed for communication to non-UK resources.)

   h. As part of the server implementation, a baseline analyzer shall be run. Any resulting recommendations shall be addressed according to risk and the decision to implement or not implement shall be documented. The baseline analyzer report and the documentation associated with any resulting configuration changes shall be retained for one year.
i. All servers and hardware shall use UKAT’s domain name and time services, if applicable. Machines in UKAT’s Active Directory environment do not apply.

8. **Local Firewall**
   a. Firewalls shall be enabled.
   b. All firewall services and ports shall be disabled or denied by default.
   c. All enabled firewall services and ports shall be documented (with justification noted and supervisory approval (i.e., recognition and acceptance of the risk.)
   d. *Any subsequent changes to firewall services and ports shall be justified and documented via the unit’s Change Management and Configuration Management processes and procedures.*

9. **SysAdmin or “Turnover” Documentation**
   a. Each server shall have its own System Administrator or “turnover” documentation that lists the particulars associated with the server such that, if the server is turned over to someone else to maintain, the new System Administrator who assumes maintenance responsibility has an informing document that explains the server’s use, settings, etc.
   b. The SysAdmin or “turnover” documentation shall contain, at least, the following:
      1) The server name,
      2) Hardware make & model,
      3) The amount of internal or external storage associated with it,
      4) Purchasing information including vendor or reseller, cost, funding source, warranty information, asset tag,
      5) Server purpose and any primary application,
      6) Enabled ports and services,
      7) Firewall configuration,
      8) Networking information,
      9) Standard operating procedures,
      10) Disaster recovery plans,
      11) Standards & policy exception documentation,
      12) Change management and configuration management process/procedure,
      13) System administrator name and contact information,
      14) Users and service accounts,
      15) Primary business owner or minimally, the name of the primary business unit needing the server,
      16) Data owners and data custodians,
      17) Attestation regarding the existence (or not) of all confidential or sensitive data, such as
         a. Protected Health Information (PHI),
         b. FERPA data,
         c. Social Security Numbers or driver license numbers,
         d. Credit card data, or
         e. Any other personally identifiable information.
IV. DEFINITIONS  (*not complete*)

V. REFERENCES

VI. REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
<th>Primary Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/08/15</td>
<td>Initial draft developed</td>
<td>M. Carr</td>
</tr>
</tbody>
</table>

VII. END NOTES