Office of Information Technology

IT Standard
SERVER CONFIGURATION AND SECURITY

Standard: IT10001
Original Effective Date: 09/21/2010
Last Revised: 07/02/2021

Last Reviewed: 07/02/2021
Next Scheduled Review Date: 07/01/2022
Version No.: 3.3
Administrative Owner: Chief Technology Officer

PURPOSE

STANDARD

Montgomery College ("College") information technology resources and digital business information are critical to the administrative business of the College and the success of its students. The task of protecting these resources according to Montgomery College Board of Trustee ("BOT") policy, Federal and State laws and regulations, and industry based regulations and compliance requirements is the responsibility of the Office of Information Technology (OIT).

The protection of College information resources requires controls to manage risks to the confidentiality, integrity and availability of College information. This standard defines controls for the management of servers that handle College information.

SCOPE

This standard applies to all servers that are connected to the College networks or contain confidential College information as defined in College Policy 31103.

DEFINITIONS

Term	Definition
Administrative Credentials	Credentials which provide a user with elevated access to a system or application in order to make configuration changes. i.e. Administrator, root, Oracle, etc. This type of credential set is also referred to as a privileged account.
Confidential Information	Defined by College Policy 66002 as: Confidential Information includes but is not limited to the following: the personnel record of any past or present employee; any record containing PII; credit or debit card data; student information which has not been identified as directory information (see Board Policy #41003 Student Cumulative Records); records or material that have otherwise been identified as confidential, subject to trademark or a copyright protection, or for which there is a contractual limitation on disclosure; records of the Office of General Counsel, or any records of which exposure unnecessarily invades personal privacy or impairs individual rights.
Primary System Administrator	An individual who is in charge of the setup, maintenance and ongoing operation of a networked server.
Secondary System Administrator	An individual properly cross-trained and capable of assuming the duties of the Primary System Administrator.
Server	Any computer, computing device, or virtual machine providing services over the college network, whether located on premise or in the cloud, is a server for the purposes of these standards, whether or

	not the underlying hardware was so designated at time of acquisition. This does not apply to individual workstations.
Systems Engineers	The OIT group responsible for implementing, administering, and maintaining centrally managed servers at Montgomery College.

STANDARD

A. Implementation

1. All server specifications will be prepared by OIT to ensure they meet College hardware standards as specified in the latest version of the Service Implementation Questionnaire. An exception will be made for specialized servers where in-depth skills exist in the user community.
2. All servers must be purchased through the OIT procurement processes.
3. Servers holding confidential information must comply with all applicable State or Federal laws and regulatory requirements.
4. Only properly licensed software will be installed on any server. All software must be installed on servers only by authorized personnel.
5. Where possible, all academic and administrative servers will be installed in local campus data centers, in the TPSS ITOC NOC, or in an OIT sanctioned and managed cloud service provider. This requirement provides both physical and security protection of the devices, ensures adequate backup processes are in place, and provides power protection for continuity of operation.
6. Before server hardware purchase or implementation, all servers must undergo an implementation review that includes analysis by a committee comprised of staff from the Network Operations Center (NOC), Network Engineering (NE), the IT Security Group (ITSG), the application owner, and any others as appropriate. Any decision to locate the server anywhere other than a managed data center (on premise or in the cloud) or to purchase physical resources must be approved by this implementation committee. If the committee is unable to reach a consensus, the CTO will review the information and provide a final decision.
7. Enterprise services (including but not limited to dynamic host configuration protocol [DHCP], domain name service [DNS], e-mail, routing, network monitoring tools [including sniffers], firewalls, e-mail relay services, and directory services) must be implemented and managed only by OIT or OIT-approved service providers.

B. Security, Security Patches and Anti-Malware

1. All servers must undergo regular periodic vulnerability scans as designated and performed by IT Security Group ("ITSG") including those performed in accordance with regulatory or compliance activities.
2. A process must be developed for each server to address and mitigate critical vulnerabilities and deploy timely patch management based upon risk to College IT operations.
3. Servers, including almost all operating systems and many software applications have periodic security patches released by the vendor that need to be applied. Processes will be developed so that patches which are security related or critical in nature should: (1) have their applicability determined and (2) if applicable, a plan for testing/deployment and/or mitigation activities, consistent with the criticality of the patch.
4. Where technically feasible, all servers must have anti-malware installed, with real-time scanning activated and signature updates performed at least weekly, and preferably daily. All applicable servers must be accessible and manageable from a central management console for the anti-malware package.

C. Configuration

1. All servers must be implemented with IT approved baseline security settings as identified by ITSG.

2. All servers must undergo a vulnerability assessment (including a vulnerability scan) designated and performed by ITSG prior to production implementation. All critical vulnerabilities must be mitigated prior to the server going into production.
3. All production servers must be monitored, at a minimum, to indicate that the server is operational. The monitoring process or application must provide results to a central management console.
4. All servers must synchronize their time with designated College timeservers.
5. All servers must use designated College DNS services.

D. Administration

1. A server must have one designated Primary System Administrator. A server must have at least one designated Secondary Administrator.
2. All servers must be accessible through administrative credentials by appropriate staff for maintenance.
3. Administrative functionality must be restricted to a limited set of trained/qualified staff responsible for maintaining and managing the server or its applications. Only users requiring privileged access will be provided administrator-level accounts.
4. Administrator accounts must be used only for tasks relating to server administration duties, not normal user-related tasks.
5. All privileged access to any server must be auditable, with clear accountability to a specific user.
6. All servers must have an active maintenance agreement in effect to provide response within one business-day. Servers must have the minimal maintenance response appropriate for their criticality, as determined by the system owner and NOC staff.
7. All server accounts, regardless of privilege, must have strong passwords and be changed on a periodic basis, as defined by the Information Technology Resource Authentication Standard. All passwords should be vaulted in a Privileged Account Management system as defined by the Information Technology Resource Authentication Standard.

E. Data Protection

1. Backup processes appropriate to the needs of the application owner and the College must be in place to support all data and information stored on the servers.
2. Any backup media containing confidential or sensitive data that is physically removed from the on premise or cloud data center must be encrypted.
3. Any server or data center storage media (disks, tapes, etc.) must have all data deleted prior to disposal. Deletion should be performed using a process specifically designed for secure purging of data from storage media and may include destruction.
4. Servers utilized in the processing or storing of credit card information must comply to the requirements of the most current PCI DSS version and as defined by the College's PCI Compliance Level.

F. Auditing

1. Server Primary System Administrators are responsible for enabling logging/auditing of events that are significant and important to the security of the servers for which they are responsible. Such events include but are not limited to:
   a) authentication events (logons, logoffs, failed logons, use of su/sudo, etc.)
   b) system events
   c) system configuration changes
2. Audit logs must collect enough information about an event to forensically examine the event. Such information includes but is not limited to:
   a) date and timestamp
   b) source
   c) activity
   d) outcome
3. Audit Logs should be reviewed regularly.
4. An audit which reveals a security issue in an event should be reported to ITSG in accordance with the Montgomery College OIT Information Security Incident Response Plan.

EXCEPTIONS

This standard is applicable as of its Effective Date. Exceptions to this standard will be considered on a case by case basis in accordance with the IT Exception Request Form.

COMPLIANCE AND RECOURSE FOR NON-COMPLIANCE

Montgomery College has established College Policies/Procedures and the OIT has established IT Standards and Processes and associated guiding documents to provide appropriate protection of technology resources, to assure protection of personally identifiable and sensitive information and to promote privacy. Any faculty, staff, contractor, or vendor found to have violated any part of College Policies, Procedures or IT Standards or Processes may be subject to disciplinary action and/or legal action.

RELATED DOCUMENTS

Acceptable Use Policy and the accompanying Procedure/Guidelines Statement

WEB SITE ADDRESS FOR THIS STANDARD

APPROVALS / REVISION HISTORY

DATE	VERSION / REVISION / NOTES	APPROVER
April 21, 2010	Original roll-out of this Server Configuration and Security Standard document.	Patrick Feehan, Information Security and Privacy Director/ITPA
September 2010, April 2016, February 2018	Revised.	Patrick Feehan, Information Security and Privacy Director/ITPA
September 2019	Reviewed.	Anwar Karim, Chief Technology Officer
September 30, 2020	Decided upon and added review cycle dates.	Nell Feldman / Keith Wilson
July 2, 2021	Minor grammatical changes and other minor points of clarification.	Anwar Karim, Chief Technology Officer