MONTGOMERY COLLEGE

Office of Information Technology

IT Standard
NETWORK OPERATIONS CENTER INFRASTRUCTURE MONITORING

Standard:	IT21005
Original Effective Date:	May 22, 2017
Revision Date:	May 22, 2017
Review Date:	December 21, 2021
Next Scheduled Review Date:	December 21, 2022
Version #:	1.0
Administrative Owner:	Chief Technology Officer

PURPOSE

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 in compliance with Montgomery College Board of Trustee ("BOT") policy and applicable Federal and State laws and regulations is the responsibility of the Office of Information Technology (OIT)

The purpose of this standard is to provide the basis by which the Office of Information Technology (OIT) Network Operations Center (NOC) will monitor the College's IT infrastructure. This standard is designed to protect the organization against loss or degradation of service by providing minimum requirements for monitoring various elements of the IT infrastructure, including but not limited to power, cooling, network, servers, storage, applications, and services. The goals of the monitoring are:

- Ensure appropriate device status data is available to the Network Operations Center;
- Provide real-time response by NOC operators to identified issues;
- Where possible, provide a centralized monitoring tool for aggregated status data collection, allowing for a correlated perspective on any issues;
- Provide access on infrastructure status to various parties, including support staff, managers, directors, and other leadership members, as appropriate;
- Where possible, provide alternative or redundant monitoring capabilities to maximize monitoring functionality even in the face of infrastructure or monitoring failures.

SCOPE

This standard applies to all IT devices and services that support the College's mission. This will include, but is not limited to:

- All production servers;
- All data storage arrays that contain production data;
- All network devices;
- Power and cooling in all College-owned data centers, campus points-of-presence, buildings MDFs, and network closets;
- Where possible, any College services that rely on IT resources for availability (such as eRadio and MCTV);
- Any College applications/SaaS (Software as a Service) that reside outside of College-owned data facilities.

This standard does not preclude the use of additional monitoring tools or processes that may be implemented as appropriate by IT staff, engineers, or administrators.

DEFINITIONS

	Term	Definition
	Server	Any computer, computing device, or virtual machine providing services over the college network 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.

	Network Operations Center (NOC)	The IT monitoring operation, manned by operators utilizing various tools that can be leveraged by other IT staff for various purposes in maintaining their infrastructure devices.

STANDARD

1. The NOC utilizes WhatsUpGold as its standard monitoring tool. WhatsUpGold supports standard SNMP protocols and should be compatible with any IT device that supports SNMP. All devices will use OIT’s standard SNMP string and be configured to point to the WhatsUpGold server(s).
2. Where possible, all production servers will have SNMP activated and reporting to the WhatsUpGold server(s).
3. Where possible, all production network devices will have SNMP activated and reporting to the WhatsUpGold server(s).
4. The NOC utilizes APC InfraXture to monitor power and cooling data in data centers and network closets. Where possible, all UPSes supporting IT infrastructure will have monitoring capabilities installed and reporting to the InfraXture server(s).
5. Where possible, devices will report a range of statuses, dependent on the type and purpose of the device. These include, but are not limited to:
   i. Servers: Heartbeat, data storage available, data storage used, memory available, memory used.
   ii. Network switch: Heartbeat.
   iii. UPSes: Heartbeat, capacity, capacity used, on battery, battery state.
6. Where possible, appropriate alerting thresholds, determined in coordination with system owners, will be activated. Initial thresholds will generate an e-mail alert. Escalating alerts will generate text messages, as well as e-mail notifications to additional staff and appropriate managers.
7. All administrators/system owners will submit contact information to be reviewed annually or in the event of transfer of ownership. This will include, but are not limit to:
   i. System owner name, office phone, cell phone, email and after hours availability.
   ii. Application owners name, office phone, cell phone, email and after hours availability.
   iii. All systems will include contact name of backups, office phone, cell phone, email and after hour’s availability.

EXCEPTIONS

Exceptions to this policy will be considered on a case-by-case basis in accordance with the IT Exceptions Request Form. All exceptions must be approved by CTO.

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, vendor or other agent 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 PROCESS

http://cms.montgomerycollege.edu/WorkArea/linkit.aspx?LinkIdentifier=id&ItemID=7331

APPROVALS/HISTORY

DATE	VERSION / REVISION / NOTES	APPROVER
May 22, 2017	Approved	Patrick Feehan, Information Security and Privacy Director/ITPA
December 21, 2021	Reviewed and added review cycle date.	Joseph Marshall, Director of Data Center Operations