SERVER REGISTRATION PROCEDURE
CATS - INFORMATION TECHNOLOGY

VERSION HISTORY

Version	Date	Author Name	Reason for Revision
1.1	7-15-2008	Mike Persina	Initial Publication - DRAFT
1.1	7-01-2010	Mike Natale	Annual Review/Minor revision to section Procedural Steps
1.1	10-4-2011	Michael Persina	Annual Review – No Changes
1.2	9-24-2012	Mike Persina	Annual Review - Updated to reflect change in procedure
1.2	9-4-2014	Ken Nelson	Annual review
1.3	9-16-2014	Mike Natale	DNS review added
1.4	1-26-2015	Mike Natale	Multiple updates - Procedural steps clarified and added, Responsibilities updated
1.4	9-6-2016	Mike Natale	Annual Review
1.4	12-1-2017	Mike Natale	Annual Review
1.4	02-01-2019	Mike Natale	ServiceNow reference added
1.4	2-20-2020	John Remley	Annual Review
1.4	9-21-2021	John Remley	Annual Review
1.4	4-21-2022	Mike Natale	Annual Review
1.4	2-23-2024	Mike Natale	Annual Review
1.4	4/29/2025	Ken Nelson	Annual Review

Commented [NK1]: Needs updated for (logging/edr/antivirus and roles/responsibilities related to pci 4.0

	Wright State University Information Security	

Controls	
Policy Title:	Server Registration Procedure
Category:	Information Technology
Audience:	CaTS Staff
Reason for Revision:	*N/A*
Created / Modified Date:	1-26-2015
Location:	http://www.wright.edu/security/policy/

Responsible Parties	
Author	Mike Persina

TABLE OF CONTENTS

Procedure Purpose

All servers placed on the WSU network must be processed through the CaTS Server Registration workflow. The purpose of this procedure is to outline the required steps within this workflow. By identifying and annotating these steps it is less likely something will be missed. IP addresses are not to be assigned to servers until a Server Registration is in place.

Procedural Steps

1. A party requesting a new server completes the "New Server Registration" process in ServiceNow: http://www.wright.edu/information-technology/security/server-registration

2. Upon completion, an automatic notification of new server request is sent to the Security group and System Admins.

3. The Security department reviews the request (*and interviews requestor if necessary*) to determine if server is expected to house sensitive data. Based on server content and function, the Security department will determine which VLAN to place server, as well as necessary router ACL and/or firewall rule changes, and level of logging to the central logging server (SIEM).

4. The Security department makes required firewall changes, and notifies the Network Engineering department if router ACLs need to be modified.

5. System Admins evaluate request to determine if local system firewalls require modification.

6. DNS names are reviewed by the Marketing department and DNS administrator.

7. Security will vulnerability scan all new servers and require remediation prior to opening to off-campus.

8. Additional services open to off-campus must be scanned for vulnerabilities prior to ports being opened through the firewall. Contact the CaTS Information Security team via email at security@wright.edu to have your server scanned.
    a. System Admins are expected to ensure that servers and associated applications are fully patched and hardening measures implemented prior to opening services to off-campus.
    b. System Admins must also ensure that unnecessary services and applications on server are disabled and/or removed.

Policy Responsibilities

This policy provides guidelines for procedures and responsibilities for management, network administrators, all users, and IT services.

☐ **Management**

- Be cognizant of the Server Registration process, and ensure employees comply with this policy.

☐ **Network and System Administrator(s)**

- Ensure registration is completed fully and accurately annotates any sensitive data touching system to be registered. IP addresses are not to be assigned to servers until a Server Registration is in place.
- Ensure that servers and associated applications are fully patched, hardening measures implemented, and unnecessary services and applications on server are disabled and/or removed prior to opening services to off-campus.
- Allow a full business day notice to allow time to process request and affect firewall policy push.

☐ **Faculty and Staff**

- Ensure registration is completed fully and accurately annotates any sensitive data touching system to be registered.
- Allow a full business day notice to allow time to process request and affect firewall policy push.