Server Audits Policy

Effective Date: November 7, 2007

Approval: December 17, 2016

Maintenance of Policy: Chief Information Officer

PURPOSE: This policy defines UDit's authority and responsibility for auditing and enforcing the security configuration of the information technology systems supporting the University of Dayton.

SCOPE: This policy applies to all computing and networking devices that make up the suite of UD-provided services whether located at UD or hosted off-campus by the University or other authorized agents.

POLICY:

UDit has the responsibility and authority to conduct audits as needed on all University systems and retains the right to enforce compliance when and where necessary.

- Individual systems will be audited periodically as outlined within UD's Vulnerability Assessment program, but more frequently if determined appropriate.
- UDit will maintain owner point of contact information and administrative/root access to every system within the Data Center.
- For premise-based systems maintained outside of the Data Center, UDit will coordinate with the system owner to gain the necessary access.
- Auditing may be performed remotely, manually, or using locally installed agents; UDit will work with system owners to ensure methods chosen do not adversely impact their operations.
- UDit will notify system owners whenever administrative/root access is used, an audit is conducted or changes are made to the environment hosting the system.
- In addition to centrally archiving audit results, UDit will provide individuals responsible for audited systems a copy of the results recommending optional and mandatory changes and, if necessary, a timetable for resolution.
- UDit will not change the hardware or software configuration of any system without the consent of the system owner unless a significant security risk has been identified.

REFERENCE DOCUMENTS:

1. ISO 27002 2013 Sec. #18
2. UD Vulnerability Assessment Program

APPLICABLE REGULATIONS:

1. Including, but not limited to: Payment Card Industry Data Security Standards (PCI DSS)

POLICY HISTORY:

Approved as Amended

December 17, 2015

Approved in Original Form

November 2007

POLICY (continued):

For systems hosted external to the University, the audit requirements outlined above will include the request and review of the results of security assessments conducted by and for the service provider.

Appeals to this process may be made through the appropriate dean or VP to the CIO. If that review is unsatisfactory, further appeals may be made to either the Provost or the VP for Finance and Administration, depending upon the nature of the server/service in question.