

November 7, 2018

MEMORANDUM

TO: State Board of Regents

FROM: David L. Buhler

SUBJECT: USHE – 2018-19 Information Technology (IT) Operating Plan

Issue

The Board is being asked to review and approve the USHE 2018-19 Information Technology (IT) Operating Plan.

Background

Every year, the Chief Information Officers from each USHE institution meet together to formulate an operational plan addressing information technology issues affecting all of the institutions. In the past, these plans have typically focused on the joint purchases of software (saving \$3.6 million each year for the institutions), security, and other joint issues that are better solved by the institutions collaborating together.

For the 2018 operational plan, the CIOs chose to focus heavily on security. Security risks and threats have greatly increased over the years, and subsequently, institutions have fallen behind in the tools, training, and people needed to mitigate these additional security risks and threats. Specifically, this year's plan includes the following:

- changes to Regents security policy R345 to allow for minimum security standards across all institutions;
- an appropriation request for standard security staffing levels, next generation network firewalls, advanced malware endpoint protection, and updated edge network equipment;
- an effort to continue leveraging USHE's size to save on system-wide software contracts, as well as share best practices for enterprise software, disaster recovery, business continuity, strategic initiatives, and business case analytics; and
- an effort to create awareness and increase maturity on electronic accessibility issues for student access and completion.

Commissioner's Recommendation

The Commissioner recommends the Board review and approve the 2018-19 USHE Information Technology Operating Plan.

DLB/KLH/SH
Attachment

David L. Buhler
Commissioner of Higher Education

2018-19 USHE IT Operating Plan

Ensure security of - and appropriate, timely access to - data

USHE R345 Regents Security Policy Changes

1. Adopt minimum security standards recommended by the USHE ISO Committee following NIST CSF, HITRUT, and ISO
 - a. Standard security staffing levels (\$1 million ongoing), \$125,000 per institution
 - b. Separate administrative credentials for systems and devices containing restricted data
 - c. Whitelisted network
 - d. Segment networks to shield restricted/sensitive data
 - d. No restricted/confidential institutional information on private devices
 - e. Encrypt all computers and servers with PII, PHI, and FERPA data
 - f. Comply with the changing compliance landscape (e.g., PCI, HIPAA, GDPR, FERPA, ITAR, GLBA)
 - g. Require annual security awareness user training for all USHE schools

Security Tools

1. Purchase and install next generation network firewalls (\$500,000 ongoing)
2. Purchase and install advanced malware endpoint protection (\$750,000 ongoing)

Network Upgrades Essential for Security

Update and capitalize edge network equipment to meet IOT, Network Access Control, and security standards (\$4.9 million ongoing)

Increase fiscal and operational efficiency across the system

- Leverage USHE's size to save on software contracts from Adobe, Microsoft, and Ellucian
- Develop and share best practices for acquisition, integration, and implementation of enterprise software
- Share and institute best practices across institutions through topical gatherings, including coordinating the following subcommittees (e.g., ISO, NISST, UTTC, UBUG) and updating their charters and directions
- Increase maturity on disaster recovery and business continuity
- Identify and align with strategic initiatives of higher education and how IT can support and bring those about to make higher education relevant for the future economy and environment
- Business case analytics

Support efforts to increase student access and completion

- Create awareness and increase maturity on electronic accessibility issues
- Compare UTTC inventory on student services applications and tools with CIO-compiled inventory on student services applications and tools, and look for opportunities to cooperate on:
 - o Strategic scheduling technology
 - o Business intelligence capability
 - o Student data analytics