

SUMMARY FOR STRATEGIC INFORMATION TECHNOLOGY COMMITTEE

DATE: January 15, 2019

TIME: 1:00 p.m. – 2:45 p.m.

LOCATION: Winder Boardroom, Park Building

IN ATTENDANCE:

Kirsten Butcher	Holly Christmas	Eric Eide	Bo Foreman	Cynthia Furse
Demian Hanks	Steve Hess	Nancy Lombardo	Harish Maringanti	Ken Nye
Wendy Peterson	Cory Stokes	Jim Turnbull	Jeremy Uffens	Thomas Wolfe
Rob White				

COMMITTEE SUPPORT: Jesse Drake, Emily Rushton

UNABLE TO ATTEND:

Cathy Anderson	Rebwar Baesmat	Melissa Bernstein	James Elder	Aaron Fogelson
James Herron	Jakob Jensen	Thomas Reichler	Colton Rogers	Ryan Smith
Jess Taverna	Howard Weeks	Jeff West	Joanne Yaffe	

AGENDA ITEMS DISCUSSED:

- Expanding campus alerts with desktop notifications
- Integrated Student Team update
- Updates to security policy 4-004
- Deprovisioning email accounts
- Anonymous network access
- Risk subcommittee report
- DUO authentication screen changes
- SITC meeting frequency
- Open floor

Expanding campus alerts with desktop notifications

Stuart Moffatt, associate director for Emergency Management Services in the Department of Public Safety, presented a proposal to expand the capability of Campus Alert, the university's mass notification system, to include notifications to desktops in student, staff, and faculty spaces on lower campus. The proposal was presented to and approved by the [Architecture and New Technology Committee \(ANTC\)](#) at its November 2018 meeting. A pilot program with a small number of campus groups/departments and IT professionals to deploy and expand the additional method will soon be underway, leveraging an existing Alertus Technologies license managed by U Health.

The committee approved the proof of concept, and asked Moffatt to report back on pilot program efforts.

Integrated Student Team update

Cory Stokes, Associate Dean of Undergraduate Studies and Digital Learning Officer, gave an update on the Integrated Student Team (IST), which he co-chairs. IST provides recommendations to SITC and Academic Senate's Executive Committee. This was an information-only item.

Updates to security policy 4-004

Trevor Long, associate director for Governance, Risk & Compliance in UIT's Information Security Office, updated the committee on upcoming rule changes to [University Policy 4-004](#) around data classification and encryption to align with recent changes to the Utah System of Higher Education's [IT Resource Security Policy R345](#). The key change in language is that encryption of sensitive data is now *required* rather than *recommended* in accordance with university rules and guidelines, with an additional reference to the USHE policy. This was an information-only item.

Deprovisioning email accounts

Corey Roach, manager for ISO Enterprise Security, presented an update on deprovisioning email accounts at the university.

The committee approved the following requests to address decommissioning user accounts in the event of an urgent termination: 1. Add a procedure to scramble the user's password so they cannot gain access to university systems; and 2. Authorize Chris Stucker, director of Identity & Access Management (IAM) to form and lead a working group to look at specific use cases and solutions surrounding account terminations.

Anonymous network access

Roach discussed two recent cases involving nefarious activities on university networks that were accessed anonymously, and proposed eliminating anonymous access of wireless networks at the university as well as revising the access method for UGuest to establish a means of identifying network connections.

The committee approved a motion to take the proposal to the Office of General Counsel (OGC), University Cabinet, and Network Architecture Community of Practice, and asked Roach to report back on his findings.

Risk subcommittee report

CISO Randy Arvay gave a report on recent activity by the U's risk subcommittee ([approved by SITC in May 2018](#)), specifically in regards to web-hosted DNS integration.

Arvay also updated the committee on an IAM project to archive inactive Active Directory-based accounts, an initiative designed to streamline centrally-administered AD-based account management and reduce risk to the university.

These were information-only items.

DUO authentication screen changes

Arvay updated the committee on an IAM project related to [recent changes to the Duo authentication screen](#). Users may now receive a one-time use bypass code to self-register a new device after answering a series of identifying questions. This was an information-only item.

SITC meeting frequency

SITC Chair Cynthia Furse proposed a change to the frequency of SITC meetings. Currently, SITC meetings are held on a monthly basis. Dr. Furse proposed changing the meeting to bimonthly (every other month), keeping in mind that meetings will generally be canceled during the months of July and December. The committee approved the measure. The next SITC meeting is scheduled for March 19, 2019.

Open floor

Committee members welcomed SITC’s newest member, Wendy Peterson, Deputy Chief Human Resources Officer.

Action summary			
Action	Topic	Person/Group	Next steps
Approved	Expanding campus alerts with desktop notification	Stuart Moffatt, Emergency Management Services	Continue with a pilot program to test the desktop alert method, and report back on its progress.
Approved	Deprovisioning email accounts	Information Security Office	Add a procedure to scramble a user’s password in the event of urgent termination, and authorize IAM Associate Director Chris Stucker to lead a working group that will look at specific use cases and solutions around account terminations.
Approved	Anonymous network access	Corey Roach, ISO Security Assurance	Take a proposal to establish network identification when accessing university networks to the Office of General Counsel, University Cabinet, and Network Access Point Community of Practice, and report back.