

College/Division Administrator Meeting – July 9, 2015

Mary E. Dickerson, MBA, CISSP, CISM, PMP

Executive Director, IT Security

Chief Information Security Officer

University of Houston | University of Houston System

phone: 832-842-4679

email: mdickerson@uh.edu

UIT Security Briefing

- **New SAMs Approved!!!!**
 - 07.A.06 - Email Retention (Formerly **MAPP 10.03.07**)
 - **07.A.07 – NEW – Employee Messaging Services**
 - 07.A,08 – Data Classification & Protection (Formerly **MAPP 10.05.03**)

SAM 07.A.06 - Email Retention (MAPP 10.03.07)

- **Defines types of Email Messages**
 - Personal
 - Transitory Correspondence
 - System/University Business Records
- **Specifies requirements to preserve messages that are Business Records**
 - Questions about classification of messages -> manager or business administrator
 - Can escalate questions to UHS Records Retention Officer

SAM 07.A.06 - Email Retention (**MAPP 10.03.07**)

- **All users expected to:**
 - Identify & preserve business records according to record retention policies
 - Delete transitory correspondence as soon as usefulness has ended
 - Not retain messages longer than required

07.A.08 – Data Classification & Protection (**MAPP 10.05.03**)

3 Levels of Data

Level 3 = Public data in the public domain

- Information readily available in the public domain
 - Information posted on the University public web site, **such as your E-mail alias**

Level 2 = Protected Information

- Information subject to disclosure or release under the Texas Public Information Act if requested

07.A.08 – Data Classification & Protection (**MAPP 10.05.03**)

Level 1 = Confidential / Sensitive / Mission-Critical

- **Confidential**
 - Social Security numbers
 - Educational records (FERPA)
 - Health care information (HIPAA)
 - Customer information (Gramm-Leach-Bliley [GLB])
 - Credit Card Numbers (PCI)
- **Sensitive (Texas Business Code) –**
 - First & last name in combination with:
 - Social Security Number
 - Government-issued ID (e.g., driver's license), or
 - Account/Credit card/Debit card number & access code
 - Information that identifies an individual and related to:
 - Physical or mental health or condition of the individual
 - Provision of health care of the individual
 - Payment for the provision of health care to the individual
- **Mission-Critical** – essential to the continued performance of the University

07.A.08 – Data Classification & Protection (**MAPP 10.05.03**)

Level 1 – **Required** Protections

- Stored on critical information resource (such as an enterprise application or network file share)
- Appropriate access controls (e.g., user ID and password)
- Must be **encrypted** if transmitted over a **wireless network** or via **email**
- Stored on **portable device** only with valid business reason & if information is **encrypted**
- Stored on **non-university device** only with valid business reason and Department Chair or Chief Information Security Officer must approve
 - **Includes cloud service providers – must have specific protections identified in the contract**

07.A.07 – NEW – Employee Messaging Services

- **Policy created by Human Resources, Office of General Counsel, and UIT**
 - Addresses Legal, Compliance, Business Continuity and Technology concerns
- **Policy Provision Highlights:**
 - Employees must use university-offered messaging services (email, IM, video chat)
 - Employees must use university assigned email alias/address for all official university business and set as their destination address in PASS.
 - Employees must use passwords or other security on personal devices if accessing university e-mailboxes
 - Employees going out on leave should set out of office/auto response messages and/or mail forwarding rules.

07.A.07 – NEW – Employee Messaging Services

- Policy Provision Highlights continued...
 - Employees may not keep their email alias or mailbox when leaving the university.
 - Employees must remove all personal messages from university mailbox prior to leaving.
 - Employees must remove all university messages from personal devices prior to leaving.
 - Employees must set out of office/auto response with appropriate UH contact information prior to leaving.
 - Employees must update PASS with a personal email address for HR communication purposes prior to leaving.
 - Incoming mail to the former employee's mailbox will not be forwarded to a supervisor. In specific cases where a business need exists, approval must be obtained from IT Security/OGC/HR.
 - Former employees may retain their email alias or mailbox if a business need exists. The department must sponsor the account.
 - Employees should contact their IT department if they have a need to email a large number of recipients (100+) from their individual UH mailbox.

07.A.07 – NEW – Employee Messaging Services

Next steps:

- Communications/awareness plan for employees
- Creation of FAQ

- Workshop being scheduled for early August
 - Review policy details
 - Discuss implementation plan and timeline
 - Answer questions

- Policy presentations/workshops for areas available by request

- Implementation will be phased in stages
 - Policy awareness is first step
 - Some processes will be handled manually while modifications are made

07.A.07 – NEW – Employee Messaging Services

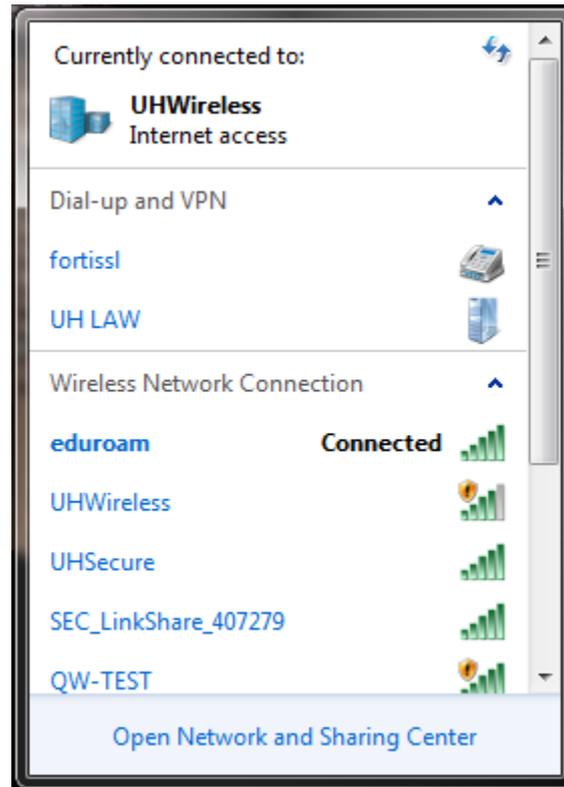
What you can do:

- Read the policy – understand the provisions
- Communicate questions
- Attend policy workshop or send a representative
- Request policy presentations/workshops for your areas
- Be patient as issues are addressed

WiFi Update

- UH Wireless Options:
 - **UHWireless** -> Visitors & Guests
 - Splash page – coming **August 3rd!**
 - **UHRegistered** available via AccessUH if necessary for some devices
 - **UHSecure** -> Students/Faculty/Staff
 - Uses CougarNet ID/Password
 - **Eduroam** -> Visiting faculty/staff from other universities

UH Wireless Broadcast Networks



Welcome to UHWireless

Acceptable Usage Policy

Use of University of Houston computing and networks, including the UH Wireless Network requires authorization. Unauthorized access is prohibited. Users must comply with University policies and all applicable federal, state, and local laws. Usage may be subject to security testing and monitoring. Abuse is subject to criminal prosecution. UH may, at its discretion, and without notice, remove, block, filter or restrict a user on the UH Wireless Network. Users have no expectation of privacy except as otherwise provided by applicable privacy laws. A complete manual of UH policies and procedures is available at <http://www.uh.edu/policies>. By connecting to the UH Wireless Network, you acknowledge agreement to these stipulations.

Public Wireless Disclaimer:

The UH Wireless Network is an unsecured network, and information transmitted over the UH Wireless Network may be visible to other online users. Users are solely responsible for taking appropriate actions to protect their private or personal information transmitted using the UH Wireless Network. The University of Houston is not liable for the loss, destruction or unauthorized access or use of information transmitted over the UH Wireless Network.

By clicking the "I Accept" button you agree to the terms stated above and access to UHWireless will expire in 24 hours.

Wifi Options

Students, Faculty & Staff: use "UHSecure"

- Fast. Uses the fastest campus WiFi network
- Simple. Select "UHSecure" from your WiFi networks
- Secure. Provides secure communications and access to campus resources using your CougarNet account

Guests: use "UHWireless"

- The University of Houston's Public (open) WiFi network — Is an unencrypted (unsecured) WiFi network
- Provides access to campus resources and Internet
- Requires user to open web browser and accept Acceptable Use Policy

Visiting University faculty & staff: use "eduroam"

- Provides secure communications
- Provides access to campus resources to visiting students, faculty or staff from participating eduroam institutions around the world
- Requires valid credentials from home institution

Register My Device

- Need to register devices that cannot “Accept” splash page:
 - Inventory Scanners
 - Gaming devices
 - Multi-functional printers
 - Smart TV w/out Roku
 - Roku
 - Digital signage, Mark Rosanes

Register device

UH Home ▾ Apply to UH Students Faculty & Staff Alumni Parents Visitors Search

UNIVERSITY of HOUSTON

AccessUH

Online Services List of Services



Welcome Brandon M Stratton!
Logged in via CougarNet ID.
Your password expires in 66 day(s). [Click here to reset CougarNet password.](#)

[Logout](#)



Help

Don't see all your services?
[Click here to refresh your icon list](#)

AccessUH FAQs

- [What is AccessUH?](#)
- [What is available through AccessUH?](#)
- [Can we access AccessUH away from campus?](#)
- [When using AccessUH, how will I know when my CougarNet password is about to expire?](#)
- [Why don't I see all the services available through AccessUH when I log in?](#)
- [More AccessUH FAQs](#)

CONTACT US

Chat with IT Support or call 713-743-1411

University Services

 <p>CougarCard</p>	 <p>Facility Work Order System</p>	 <p>Faculty/Course Evaluation</p>	 <p>Gartner</p>
 <p>Get Involved</p>	 <p>Office 365</p>	 <p>PEAR Student</p>	 <p>Parking Self-Service</p>
 <p>Register My WiFi Device</p>	 <p>Skillport</p>	 <p>Skillport - Books</p>	 <p>Software Download</p>
 <p>T.A.P. Employee Online Training</p>	 <p>myUH Self Service</p>		

uhregistered home screen



UNIVERSITY of HOUSTON

Welcome Brandon (bmstratt)

[logout](#)

NAVIGATION

[My Registered Devices](#)

[Register A New Device](#)

[How do I use uhregistered](#)

I WANT TO...

[Administrator control panel](#)

[Go to the UIT homepage](#)

"uhregistered" WiFi Registration

Devices Registered

Below you will find a list of devices that you have registered on the "uhregistered" network. **You may at any time remove a device that is no longer in use.**

A device that you may need to register is your Roku, game console or wireless printer. Devices will remain active on the network for up to one year. It is not necessary to register computers or smartphones.

Roku
B0-A7-37-0D-90-3D
WiFi test Roku in office

Status: enabled
Expires: 07-15-2015

[remove](#)

Television
F8-04-2E-05-33-23
TV in break room

Status: enabled
Expires: 07-15-2015

[remove](#)

[+ Add Device](#)

QUESTIONS?