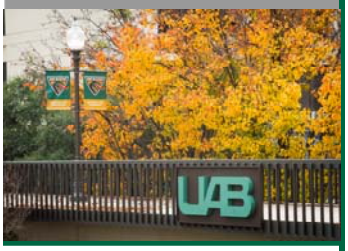
October 2016

In this issue:



University Compliance Office
AB 1120G
701 South 20th St.
Birmingham, AL 35294
Phone: 205-996-6540
www.uab.edu/compliance
www.uab.edu/policies

Compliance 411 is a quarterly newsletter published by the University Compliance Office at The University of Alabama at Birmingham. We welcome feedback and suggestions from the UAB community. Please email compliance@uab.edu to join our distribution list.

Objectives of *Compliance 411*:

- To raise awareness
- To communicate important developments
- To foster transparency

411 Compliance

THE UNIVERSITY OF ALABAMA AT BIRMINGHAM
Knowledge that will change your world

Going Limitless: UAB's Bold Approach to Information Technology

Chief Information Officer Curt Carver has set ambitious goals for UAB Information Technology to support UAB's overall mission to become an international powerhouse of research, innovation, and service.

"My vision for UAB IT is a world-class IT organization that effectively balances cost efficiency, agility, and innovation. In ten years, we will not only catch up with the rest of the world in terms of performance, but we will pass them so that we are creating best-in-class practices and are engaged in the national conversation on how information technology can transform higher education."

UAB students, faculty, and staff will soon have access to unlimited email, unlimited data storage, and 100 gigabits per second (Gbps) bandwidth to allow UAB community members to focus on their disciplinary expertise. As we evolve from an era of scarcity to a new era of abundance, UAB is transforming its approach to information technology in ways that will provide members of the UAB community with the power to execute tasks more quickly and to work more efficiently across systems. As Carver says, "We want to empower greatness in others."

But how does UAB address important information governance and data security issues while achieving these goals? While greatness in others sounds awesome, how can UAB's digital citizens change the world securely and safely?

IT data security imperative: Create a secure computing environment

Students, faculty, and staff are at greater liberty to foster new, innovative ideas when they are sure their information is secure. Protecting users and devices and managing risk are at the heart of this imperative.

Continued on page 5

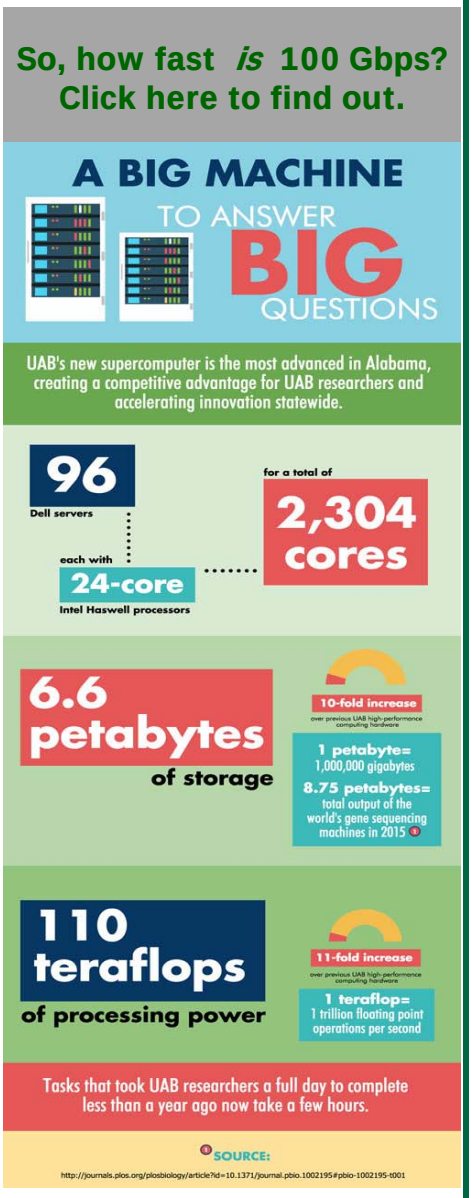


Image courtesy of University Relations

Meet UAB's New IT Security Leader Brian Rivers: Zen and the Art of IT Security

In the corner of a grey, unassuming building on University Boulevard, there is a bare office outfitted with little more than office furniture and boxes. With the exception of two framed photographs of his children, Brian Rivers' desk is free of the paper jetsam you might expect of a busy executive. UAB's new Chief Information Security Officer simply hasn't slowed down to unpack. No matter -- this pragmatic environment works well for someone whose goals for keeping information systems and data secure are simple, human-centered, and focused on empowering the people he congenially refers to as his customers. Since his arrival from Athens, GA in July, he has gone straight to work considering how he can make information security easier and more efficient for UAB students, faculty, and staff.

> "Our customers should be able to easily consume what we communicate to them. Complex messages are barriers to workflow and timeliness; we want to remove those barriers."

With ever-present, evolving challenges to maintaining security and integrity of data come many policies, standards, procedures, and guidelines that are intended to inform everyday users about how to conduct their daily work in teaching, research, and service. But Brian and his team want to accommodate human nature rather than expect every individual to memorize numerous requirements and restrictions. It's their philosophy that resources need to reflect what we know about our faculty, staff, and students' day-to-day activities, and also about human nature in general.

"A central theme of our strategic plan is simplified, direct communication," Brian explains. "Our goal is to make complying with security requirements as simple and straightforward as possible. That will require that we convey important security information campus-wide in basic ways that are easy to understand. Our customers should be able to easily consume what we communicate to them. Complex messages are barriers to workflow and timeliness; we want to remove those barriers."

Data classification system

The first step has been to establish a consistent data classification across the UAB enterprise. The new classifications will more accurately represent the nature of data we handle every day and the controls necessary to secure them.

Data classification also allows UAB to identify exactly where the risks are and to more clearly articulate roles and responsibilities, allowing funds to be redirected to processes that have the greatest need. For instance, time and cost associated with protecting all hard drives will be saved when computers that don't handle sensitive information no longer require encrypting.

Brian Rivers, Assistant Vice President for Information Security/Chief Information Security Officer, began his service at UAB in July 2016.

Brian considers this data classification to be a win-win for both users and UAB IT security. Data classification will focus UAB's investment in the right places. Stratifying data removes burden for certain faculty and staff so that they are no longer hampered with unnecessary security controls. Some data don't need protecting. Identifying data that fall into this category will "free up" much information access for students, faculty, and staff. For example, information that has been de-identified within HIPAA regulation may fall into a tier in which researchers can operate with more autonomy. On

Continued on page 4

THE UNIVERSITY OF ALABAMA AT BIRMINGHAM
Knowledge that will change your world

Compliance Challenge

Do you think a breach of the Family Educational Rights and Privacy Act (FERPA) occurred in the scenario below? Click on an answer A.-E. to enter a drawing for one of two $10.00 Mooyah gift certificates to be held Dec. 5, 2016. Only individuals with addresses ending in uab.edu/uabmc.edu qualify.

Anthony personally calculated his final course grade to be 91/A. To his surprise, his professor calculated a final grade of 89/B. In an effort to resolve the discrepancy, he emailed Professor Burns from his official UAB account to request the details of his grade calculation. Professor Burns promptly responded by emailing Anthony a spreadsheet containing grading detail for the course, including each enrolled student's name and his/her scores for quizzes, exams, and other assignments. Anthony opened the attachment to check his grade and immediately notified Dr. Burns that he had received course grades for all of his classmates in error. He then deleted the email and the attachment.

Based on the facts presented above, which of the following is true?

A. Anthony caused a FERPA breach by merely requesting information about his grade through email.

B. Exchanging with Anthony through official UAB email account about his grade would have been allowable, but Dr. Burns caused a FERPA breach when he emailed grading detail with his classmates' identifying information to Anthony.

C. Anthony avoided a breach when he immediately notified Dr. Burns that he received detailed course grades for all of his classmates in error and deleted the email and attachment.

D. No harm was done because Dr. Burns didn't intend to send Anthony grading detail for all the students.

E. Dr. Burns never should have used email to communicate with Anthony about his course grade under any circumstance.

See a Suspicious Looking Email? Just PhishMe!

One of UAB IT's top strategic imperatives is to create a secure computing environment. It's relatively easy for an attacker to compromise an institution by gaining unauthorized system access via phishing. Industry experts report that 91 percent of all security breaches start with phishing emails. Recently, in a single week, over 50 such breaches were experienced at UAB, and at the rate of nearly $10,000 to assist one user in recovering from an attack, establishing a fast, simple way to recognize and report suspicious emails is critical.

Reporting suspicious messages used to be a time-consuming, multi-step process requiring copying and pasting email headers, zipping files, and emailing them to IT for evaluation. Enter PhishMe, an information security company with which UAB has contracted, that provides technology to help employees report potential phishing emails with a single click, thus giving UAB IT the means to shut down attacks as soon as they happen.

To enable the one-click PhishMe solution in your Outlook, follow the instructions at **https://www.uab.edu/it/home/images/InstallingPhishMeReporterfromSoftwareCenter.pdf**. When you see an email that doesn't look like legitimate business to you, all you have to do is click on the PhishMe icon in your toolbar, and IT will be notified immediately.

Examples of typical phishing emails can be messages that:

* Ask you for your password;
* Demand payment for a parking ticket or other such payment;
* Inform you that your child be will suspended from school for failure to pay; or
* State that an account has been frozen until you click on an approval link.

PHISHME

Other characteristics to keep your eyes out for:

* URLs without the 'https:' prefix;
* Low-quality images that appear to be stretched or that violate branding guidelines;
* Domain suffixes that do not match the ones with which you're familiar; and
* Browser warnings that it is unsafe to proceed.

If it has any of the above — or just looks dubious to you in general — it's probably worth reporting. For more information, visit **UAB IT's webpage on phishing**.

Brian Rivers

Continued from page 2

the other hand, classifying more sensitive data into a separate category fosters clarity since there will no longer be any doubt as to whether it can be shared.

Brian and his team want to empower individuals with information to make responsible choices within the data classification standard. "It's as important to know when we aren't restricted by regulations as it is to know when we are." Sometimes that means providing alternatives that will make work more productive. "It's important to understand where outliers exist so that we can evaluate exceptions, but current exception processes can be cumbersome." In the near future, exception approval processes will be clear and more user-friendly.

Dual-factor authentication and single sign-on

Dual-factor authentication is a security technology that helps protect login credentials. Many employees today are at risk of password theft via Phishing and other types of attack. Dual-factor authentication strengthens login credentials by adding another way of determining that the person with your password is actually "you". It typically uses a factor that can't be easily given away, like a code sent to your phone or a physical token you carry with you.

Along with increasing security, dual authentication does also increase barriers to access. However, UAB is looking to address this increased burden with single sign-on. Using single sign-on technology will reduce the number of times users have to log in to various UAB systems. It remembers users as they move from system to system.

These two techniques work well together to protect against stolen passwords and to reduce the number of times users have to submit passwords.

IT policy and the road ahead

"IT policies should be practical and actionable. We must communicate requirements with the needs of our audience in mind." To support UAB users, Brian would like to build in interactivity by allowing users to ask questions and get answers in the moment while viewing the IT policies. "Answers shouldn't be buried three-levels deep. We want to make sure help is only one step away."

According to Brian, FAQs, mouse-over graphics, and crowdsourcing sites, in which UAB community members are engaged in discussion and exchange, should be the models moving forward. Complementing such interactive policies will be one-click access to just-in-time training that immediately follows a user action that might suggest there are questions about what to do next.

The goal of IT security is to empower individuals to incorporate sound decision making into their daily work with information. This sort of cultural transformation begins at the top. "It's important that we convey a helpful tone to everyone – not a sense that anyone is playing 'gotcha'. It isn't possible for thousands of students, faculty, and staff to consume every requirement and remember it all. We want to set them up for success wherever possible by first creating awareness, and that awareness matures into personal accountability for IT security."

IT security risk management is everyone's job, and with the advocacy of CISO Brian Rivers and the customer-driven philosophy of his team, UAB can expect a less reactive, segmented system and more opportune, proactive, universal information security that works across platforms for UAB as a whole.

Code of Conduct Corner

Standard of Conduct:
Use Confidential Information Responsibly

UAB community members are creators and custodians of various types of confidential and proprietary information. Each UAB community member is required to comply with federal and state laws and regulations, agreements with third parties, and UAB policies pertaining to the use, protection, and disclosure of such information. UAB community members are expected to:

* Learn and follow all laws, UAB policies, and agreements with third parties regarding access, use, protection, disclosure, retention, and disposal of public, private, and confidential information;
* Respect the privacy of all information records, whether student, employee, or patient;
* Follow document retention and disposal policies;
* Maintain information security using appropriate electronic and physical safeguards; and
* Fulfill applicable requirements when one's relationship to UAB is terminated.

Going Limitless

Continued from page 1

Eliminating the fear of external threats by developing fast incident response protocols, strengthening user authentication, using common core security products, such as PhishMe (see page 3), Keeper (see page 6), and establishing a clear data classification system (see page 2) enable business continuity and allow students, faculty, and staff to focus on research, educational, and administrative endeavors and to do so confidently and efficiently.

EMPOWER UAB: YOUR UAB IT STRATEGIC PLAN

IT information management imperative: Establish shared governance

Additionally, UAB IT is committed to engaging stakeholders in the process of building policies, procedures, and processes used to manage information. Shared governance is vital at a large institution such as UAB, where various academic and research "regions" share common regulatory, risk, and operational requirements. Shared governance also promotes trust, confidence, and accountability while strengthening the organization through collaboration.

As UAB realizes its vision of international excellence, a world-class IT organization is required to steward and enable its unlimited information domain. UAB IT is committed to fulfilling its responsibility by empowering UAB community members with the tools necessary to protect and optimize information within these vast resources.

Congratulations to Compliance Challenge Winners!

Congratulations to July 2016 Compliance Challenge winners Meg Bruck, School of Health Professions, and Jim Cimino, MD, UAB Informatics Institute. By participating in the Compliance Challenge, they were entered into a drawing, and each won a Starbuck's gift certificate. To participate in this month's Challenge and enter a drawing for one of two $10.00 Mooyah gift certificates, see page 3 of this issue of *Compliance 411*.

L to R: Katie Crenshaw, Associate University Compliance Officer, University Compliance Office, and Meg Bruck, Project Manager II, School of Health Professions, Health Informatics Program

Upon emergence from the Harrison Tower informatics vault, Jim Cimino, MD, Director, UAB Health Informatics Institute, is congratulated by Suzanne Bradley, Compliance Administrator, University Compliance Office.

Effort Reporting Policy & Procedure Changes

After review and input from campus stakeholder groups, UAB's Effort Reporting Policy & Procedures have been updated to reflect regulatory changes in OMB's Uniform Guidance. The final approved version will be published soon. Please see the table below for important changes.

Previous	Effective with effort reports for periods beginning October 1, 2016
Exempt employee *approves his/her effort; PI certifies employee's effort*	Each exempt employee will *certify his/her own effort*
Effort recorded to within two decimals	Effort rounded to integer (no decimals)
Effort reporting by object code group	Effort summarized by account
Uncertified effort reports considered *past due at 60 days after end of quarter; delinquent upon generation of next quarter's effort reports*	Uncertified effort reports considered *delinquent 60 days after end of effort reporting period (No distinction between past due vs. delinquent)*
Effort reporting is quarterly	Effort reporting will be semi-annual for periods beginning October 1, 2016 (Oct-March, April-Sept)
Training must be completed before effort can be allocated to extramurally	New training required by all investigators and DEOs, then refresher training every three years

Holiday Heads Up: Alabama Ethics Law and Receipt of Gifts

Throughout the year and especially during the holidays, UAB employees should be mindful that Alabama law restricts items they may receive from vendors. As a public employee with expectations of appropriate stewardship, a UAB employee may not use their position to reap private gains or receive special benefits as a result of purchasing decisions. This includes gifts, entertainment, and personal use of promotional rebates on supplies purchased for UAB.

However, items of *de minimis* value—such as greeting cards, plaques, or other items intended solely for presentation, promotional items commonly distributed to the general public, and items that have no resale value or value to others — are permissible under state law. The statute defines *de minimis* as a value of $25 or less per occasion with an aggregate of $50 or less in a calendar year from a single provider.

Before accepting a personal gift from a business partner, employees should find out whether it is allowed by state ethics law and school or unit policy on receipt of gifts.

If it is not permissible, it should be declined and returned it to the donor, the donor market value should be paid market value for it, or it should be given to an appropriate charity through the UAB Development Office. Within reason, consumable items that may be shared among co-workers, like a tin of cookies or popcorn, may also be placed in a common break room to minimize any personal benefit.

For more information, visit **the University Compliance Office's Alabama Ethics Law webpage**.

Keeper Reduces Password Overload to a Single Character String

While it's definitely not a good idea to post sticky notes in the office to help keep up with usernames and passwords, many of us probably have some method of helping us remember the numerous passwords required to access the websites, apps, and systems we frequent.

No matter how you currently keep up with your passwords, UAB Information Technology has implemented a new solution for maintaining usernames and passwords for both professional and personal purposes. This campus-wide core security product, known as Keeper, is a password management application that stores your login credentials for different websites so that they're easily accessible to you while still being stored securely when not needed. Instead of having to remember all of your login credentials, you need only remember one master password to your Keeper Vault.

In efforts to strengthen overall information security, UAB IT strongly encourages UAB staff, students, and faculty to create a Keeper account **by registering with Keeper here** and establishing your vault at your earliest convenience. For more information and details, visit **UAB IT's Keeper webpage**.

Unlimited Storage Space with UABbox

Earlier this year, UAB IT released a new option for unlimited storage with UABbox. While space is unlimited, there are currently restrictions on the types of data recommended to be stored in UABbox (for example, sensitive data). As the new data classification standard rolls out, those restrictions may change, so stay tuned for more information. Refer to the "Welcome to UABbox" folder inside your UABbox account, or to Guidance for the Use of Cloud Services.