Dear Colleagues,

Compliance and customer service. Strategic planning and attention to day-to-day operations. Some of our activities during the past quarter illustrate how we try to keep our sights on all these objectives simultaneously.

In the fall, Dean Murray asked the Research Administration team to meet with colleagues from across the university and re-examine collectively the customer service aspect of our grant and contract management. A dozen SEAS members, including three faculty members, area administrators, faculty assistants, and research administration staff met in two half-day retreats. The first meeting was on internal SEAS processes. The second session, in which colleagues from OSP and OTD also participated, examined the research administration process from beginning to end. We came up with a number of action items to ensure transparency in the process, enhance communication, remove redundancies, and ultimately improve the research administration experience for the SEAS community.

With the arrival of Tim Bowman, SEAS’ new Executive Dean for Administration, we are refining the plan to position SEAS financially for the next decade. At the same time, we are responding to the University’s enhancements in accounting and reporting by reinforcing and reorganizing the Finance staff. SEAS’ new Controller, Tom Nawabi, will help to strengthen the accounting, card services and reimbursement, payroll, and procurement areas. As a next step, we plan to add some capacity in budget and planning.

Another unit that we are strengthening with the leadership of SEAS two executive deans, Bowman and Habbal, is Information Technology. While Indir has stepped into the role of Interim IT Director to keep the proverbial train running, the School’s leadership is focused on a longer term strategy for IT.

Finally, we continue to build the Information Security program at SEAS through assessing our current situation, building awareness, and responding to incidents. Thank you to everyone who has completed a survey or provided information on our current state.

This issue of the newsletter contains various reminders and updates. I encourage faculty members to read about gift processing guidelines, card services and reimbursements, and effort reporting. Please ask your researchers and graduate students to review information about registering for a conference. We urge everyone to pay attention to the update on the University fraud policy and to check out interesting tips about securing mobile devices and avoiding phishing scams.

Harry Dumay, PhD MBA
Chief Financial Officer/
Associate Dean for Finance and IT Operations

Staffing Announcement

After a long search, Tom Nawabi was selected to be the new Controller at SEAS. His starting date was March 19. Tom supervises accounting, payroll, procurement, and reimbursement/card services.

Tom can be reached at tnawabi@seas.harvard.edu or by phone at 617-495-1248

Indir Avdagic, who has been working at SEAS for the past 8 months as SEAS’ Information Security Officer, has accepted to be SEAS’ Interim Director of IT, in addition to his role heading the information security program at SEAS. Indir continues to report to Harry.

IT Announcement

SEAS IT/Information Security Brown Bag Presentations and Demos Series

Beginning in April 2012, SEAS IT and Information Security will launch a series of regular brown bag presentations and demonstrations of IT and Information Security Service.

The series will kick off on Thursday, April 5th at noon in Pierce Hall 100F, with “Secure File Transfer and Collaboration Tools” as the initial topic.
Information Security

Keeping Mobile Devices from Getting Lost or Stolen

Laptop computers, smartphones and tablets define convenience and mobility. They enable us to work from home, a hotel room, a conference hall, or a coffee shop. Maybe you’ve taken steps to secure the data on your mobile device: You’ve installed and updated antivirus software. You protected your information with a strong password and encrypted your data, and you’re too smart to fall for those emails that ask for your personal information. But what about the mobile device itself? Did you know that every 53 seconds a laptop is lost or stolen somewhere in the world? Chances are you’ve heard stories about stolen laptops on Harvard campus from friends and colleagues. Since the beginning of this year we had two stolen laptops in SEAS buildings. A minor distraction is all it takes for your mobile device to vanish. If it does, you may lose more than an expensive piece of hardware. The fact is that sensitive and valuable information in your mobile device may be much more valuable.

OnGuardOnline, a website managed by the federal government provides do’s and don’ts when you’re out and about with your laptop:

Do: Treat your laptop like cash; Lock your laptop with a security cable; Consider carrying your laptop in something less obvious than a laptop case.

Don’t: Leave your laptop unattended — even for just a moment; Leave your laptop in the car; Keep passwords with your laptop in its case.

For newer Mac laptops and iPhones/iPads/iPods Touch SEAS Information Security Office provides step-by-step procedures that explain how to install FREE software that can locate your stolen mobile device on a map, display a message on the screen, play a sound at full volume (even if your device is set to silent), remotely lock or remotely wipe stolen mobile devices at: https://intranet.seas.harvard.edu/information-security/information-security-tools/mobile-devices-tools/iphone

There is also inexpensive similar software for Android device, like Lookout. More information about this software is provided at: https://intranet.seas.harvard.edu/information-security/information-security-tools/mobile-devices-tools/android

If your mobile device is stolen at work, report it immediately to the Harvard University police at 617-495-1212, as well as SEAS Information Security Office at 617-496-3502 or send an e-mail to security@seas.harvard.edu. If it’s your personal laptop and you fear that your information may be misused by an identity thief, visit http://ftc.gov/idtheft for more instructions.

IT Operations

How to Avoid Phishing Scams

E-mail is one of the primary ways we communicate. We use it not only every day for work, but also to stay in touch with our friends and family, do online shopping. Since so many people around the world depend on e-mail, it has also become one of the primary methods cyber criminals use for attack. Phishing is one of the most common e-mail based attacks. Since we recently had well-crafted phishing attacks at SEAS, this newsletter tries to explain steps you can take to protect yourself from phishing attacks.

Phishing is a technique in which users are directed by an official-looking e-mail to provide personal information under false pretenses. A phishing attack begins with an e-mail pretending to be from someone or something you know or trust, such as your bank or your favorite online store. The information requested may be a credit card number, social security number, ATM PIN number, password or other personal information. These e-mails then try to entice you into taking an action, such as clicking on a link to official-looking web site, warned that failure to do so may result in a discontinuation of service, opening an attachment, or responding to a message. You should treat these messages like spam and delete them.

The main objective of phishing attacks is to harvest sensitive information about you, or gain control of your computer through malicious links or malicious attachments.

If after reading an e-mail you suspect it is a phishing attack or scam, simply delete the message. Here are some best practices for avoiding phishing attacks:

http://www.people.fas.harvard.edu/~donnelli/finance/spr12.html
- Be suspicious of any e-mail that requires immediate action or creates a sense of urgency.
- Be suspicious of grammar or spelling mistakes, most businesses proofread their messages very carefully.
- Be suspicious of attachments and do not click on links in suspicious e-mails.
- Just because you got an e-mail from your friend does not mean they sent it. Your friend’s computer may have been infected or their account may have been compromised. If you get a suspicious e-mail from a trusted friend or colleague, call them to confirm that they sent it.

There is no way SEAS IT can monitor, filter or discover all the various phishing scams that our users may receive, so be forewarned and ready when you receive these types of solicitations. Ultimately, using e-mail safely is all about common sense. If something seems suspicious or too good to be true, it is most likely an attack. Simply delete the e-mail.

If you see a phishing attack that specifically targets the Harvard University or SEAS, please contact SEAS IT at 617-495-9050 or SEAS Information Security Office at 617-496-3502.

SEAS IT/Information Security Brown Bag Presentations and Demos Series

Beginning in April 2012, the SEAS IT and Information Security will launch a series of regular brown bag presentations and demonstrations of IT and Information Security Service. These sessions are open to the SEAS community, and will provide an informal setting for participants to hear more about current and incoming IT and Information Security projects and services, learn about IT and security systems and tools, discuss best practices and helpful hints, and ask any questions you may have on a particular topic. Beverages and cookies will be provided. The series will kick off on Thursday, April 5th at noon in Pierce Hall 100F, with “Secure File Transfer and Collaboration Tools” as the initial topic. Please contact Indir Avdagic or go to registration link if you are interested in attending this event. In addition, you can find more information about tools that will be covered on the initial session at SEAS IT web site.

Accounting

Harvard University Fraud Policy

Effective 12/1/2011, the University issued a Harvard-wide Fraud Policy. The policy was developed to:

- Raise awareness of fraud
- Define roles and responsibilities for detecting and preventing fraud
- Reinforce personal responsibility and accountability
- Detail the procedures for reporting and investigating suspected fraud
- Better understand the limitations in existing control procedures that allow fraud to occur.

The fraud policy has been posted on the policy website at http://vpf-web.harvard.edu/ofs/policies/documents/fraud_policy.pdf

SEAS will be initiating a fraud policy rollout plan in the upcoming months to better inform the community about the policy.

The School of Engineering and Applied Sciences (SEAS) Gift Processing Guidelines

In December 2011, the Fall/Winter 2011 Finance, IT Operations & Information Security E-News provided SEAS gift processing guidelines for current use gifts. In this edition of the newsletter, Finance thought it would be helpful to provide additional information about SEAS 15% gift assessment fee.

This rate is applied monthly based on the prior month’s operating expenses. The assessment considers financial activity on object codes 6000-8999, excluding student aid charges in object codes 6140, 6410, 6430, 6440, 6441, and object 8922 (where the administrative charge itself will be posted).

The Administration Assessment fee is a consistent fee that is applied to current use gifts from donors at...
Harvard.

If you have any questions please do not hesitate to contact Rebecca Hegarty (617/496-4407) and/or Diane Harwood (617/495-2859) in SEAS accounting unit.

Payroll

The soft implementation of the upgrade to PeopleSoft 9.1 is currently underway and proceeding according to plan.

All Time Administrators and Time Adjusters need to complete the on line training before the go live date of April 23, 2012. The training provides a excellent overview of the changes of the time reporting screens and approval deadlines associated with the payroll process. You can access this course by going directly to Eureka.

Budget

SEAS Budget Office submitted the School's FY13 proposed budget to Harvard's Central Budget Office on March 2nd. After all the Schools submit their budgets, the University Office of Financial Strategy and Planning (OFSP) aggregates all units' budgets and presents the University Budget to the Corporation for approval.

In the next few weeks, Executive Dean Tim Bowman, CFO, Harry Dumay, and Assistant Director of Budget, Matt Preston will meet with all budget managers. The purpose of these meetings is to further understand and refine our FY13 submission.

After the Corporation approves the upcoming year's budget, schools are notified of their budget approval. Notification to SEAS Budget Managers about their Final FY13 Budget will be given officially in June and spending against their budgets will commence as of July 1st.

We also recently completed the FY12 second quarter forecast budget and Interim Reporting templates for Harvard's Central Budget Office. SEAS Budget Office worked closely with budget managers to forecast our projected financial position at the end of the fiscal year, June 30, 2012 and report on that information to the Central office.

Both the FY13 budget and the FY12 Forecast budget were a huge undertaking and were made a success by the great collaborative efforts of all the SEAS Budget Managers. We welcome any suggestions or comments on ways to improve the budget process going forward.

Card Services and Reimbursements

Travel and Entertainment Card Policy

In response to questions that are frequently asked of the travel reimbursement office, we provide this brief review of Harvard's Corporate Card program.

Corporate Card Program

The Corporate Card is the primary payment vehicle for all travel business expenses incurred by Harvard employees. It provides travelers with a variety of benefits and allows the University to capture travel data that is vital for management reporting and vendor negotiations.

Eligibility

Full time, paid, benefit eligible employees who will take three business trips per year and/or incur greater than $5,000 in entertainment expenses.

Appropriate Use of Corporate Card

Expenses charged to the corporate card should only be those of the employee for air and rail travel, lodging, car rental, meals, entertainment and business travel miscellaneous expenses. No expenses for non-employees or family members should be charged to the university corporate card.

Please see the full Corporate Card policy for more information.

New Citi Corporate Card Dispute Process

We wanted to bring to your attention a new credit card dispute procedure which eliminates paper forms and makes it easier to initiate a claim. Now you can save time and streamline your paper process by initiating a dispute over the phone.

What's New?

Now, when you call Citibank Customer Service to initiate a transaction dispute, the Citi Customer Service Representative can collect details for a dispute directly over the phone. In most cases you no longer need to complete a paper form and fax or mail it back to Citi for processing.

Benefits to You

Timeliness: By completing your claims over the phone, and providing information validation via secure e-mail, you're saving time leading to quicker resolution!

Verification: Now you'll have a confirmation e-mail for your records confirming that Citi has received all your information in order to process your claim.

Paperless: Using this new, automated process will positively impact the environment by cutting down the use of paper per claim.

Learn More

To learn more about the benefits of the new credit card dispute process: click here to access an overview, click here to view frequently asked questions and answers.

Registration Fees for a Conference

Documentation for registration to be acceptable as proof of purchase needs to include the following:

- Name of attendee
- Name of conference
- Dates
- Amount paid
- Proof of payment (credit card statement, receipt or cancelled check)

If you have any questions regarding acceptable forms of receipts of any kind please contact Noemis Ortiz (617/496-3625) or Hera Daldalian (617/495-4429).

Procurement

HCOM
Book and media vendor is now available in HCOM Marketplace:
Complete Book & Media Supply is now set up as a punch-out vendor within the Marketplace. Highlights include: free shipping for all orders over $15, additional discounts available on most bulk orders, assistance in obtaining hard-to-find titles.

Procedures/ Reminders
Changing and cancelling non-catalog requisitions: Only the original requestor can initiate a change/cancellation request. Instructions are available here. Marketplace orders cannot be changed or cancelled using this feature.

Important: Please do not make changes to an order via the phone/email without updating the PO. It causes significant delays in payment to the vendor.

- An updated iProcurement Authorization Form is available on the intranet. To set up a new user with access to HCOM, please complete it and send to Joanna Curry. Please be certain the person you're requesting access for has an active Harvard appointment and that the form has been signed by the PI.
- When creating a purchase requisition please make sure that you include your name, lab location, and the room number in the proper fields to ensure timely delivery.
- As always, please remember to receive your orders in iProcurement as soon as they have been fulfilled and delivered to you. Prompt receipt ensures that no late fees are applied to the invoice and we can take advantage of available discounts.

Research Administration

Effort Reporting: Reminder and Update
Several of our peer institutions have undergone audits and investigations by federal agencies recently, with a particular focus on effort reporting – some resulted in financial penalties and funding disallowances. To minimize Harvard’s exposure in the event of such an audit visit to our campus, we need to comply with Effort Reporting Policy in all of its aspects, with a participation level of 100%. Please remember to return the signed effort report to Bill Rasschaert before it is due, ordinarily 30 days from when you receive the form.

For the past 12 months or so, the University-wide group of sponsored research administrators has been working on an initiative to automate effort reporting and salary certification via a new University wide system. Harvard Effort Reporting and Salary Certification Initiative (HERSCI) meets biweekly to refine technical requirements for a new electronic system while major decisions are guided and approved by an Executive Committee which meets every other month. SEAS participates in the initiative as a member of HERSCI group, attended vendor demo over the summer and this spring, and conducted Focus Group with a group of faculty assistants. While this initiative is underway, please remember that we continue to utilize paper-based monthly effort certifications for non-faculty and electronic annual salary certifications for faculty.

If you have any questions about this initiative or about SEAS local process, please contact Seedang Simonin.

NIH Salary Cap FAQs
NIH has issued updated FAQs related to implementation of the new NIH Salary Cap, Executive Level II.

Inflationary Increases for Future Years
NIH inflationary increases for future year commitments will be discontinued for all competing and non-competing research grant awards issued in FY 2012, however adjustments for special needs (such as equipment and added personnel) will continue to be accommodated. Please see the full NIH notice.

Audit

Harvard's FY11 A-133 audit has been submitted to the federal government and it is posted to the OSP web-site. The A-133 audit is conducted annually by external auditor – Pricewaterhouse and Coopers, LLC. There were no findings from SEAS for the FY11 fiscal year. The FY12 A-133 audit season will begin sometime later in the Spring. As a reminder, if you are contacted directly by a sponsor about any audit, please contact your portfolio manager asap. Our office will work directly with OSP and the sponsoring agency to understand and define the scope of the audit and provide information or documentation as appropriate.