American University of Beirut
Office of the President

Dear Members of the AUB Faculty and Staff,

As you will remember, in the wake of issues raised last spring regarding the process of data review (specifically email) related to a fraud investigation by the Internal Audit department on campus, I convened a working group to assess the technical aspects of the process employed by Internal Audit and to provide recommendations for improvements. The working group consisted of five professors from FEA and FAS who have technical expertise in this field: Drs. Ayman Kayssi (chair), Zaher Dawy, Mazen Ghoul, Imad El-Hajj, and Alan Shihadeh. I wish to thank them all for long hours of work undertaken last summer and even into the fall and winter, on behalf of all of us at AUB.

Specifically, the charge for the Group was as follows, which you will also find cited in the attached report: "Review the protocols, policies, and procedures of the university's Information Technology organization as they relate to the protection of e-mail database and archive integrity, including encryption, chain of custody and related matters. Additionally, the Group will review the university's current technical environment as it relates to the need to protect the privacy of data while conducting highly targeted confidential access to the university's e-mail database and archives by authorized individuals granted such access by the President, and will recommend such measures as may be appropriate to ensure the integrity and security of the university community's confidential data."

As its review continued, I felt it necessary to give the Group a greater degree of privileged access to persons involved in the original investigation, to better understand the non-technical side, since the policy environment was key to guiding the actions of the personnel involved. In the context of approved and authorized fraud investigations that were still ongoing, the information available to the Working Group on specific aspects of the investigative methods and other topics was necessarily limited. The conclusions of the Group must be understood with this caveat in mind.

Before addressing individual points addressed in the report, let me say first that I agree with its conclusions and recommendations. They have been incorporated into the draft of the new Policy on Data Privacy that has been debated and endorsed by the University Senate and is now before the Audit Committee for formal approval. I would like to note that, ironically, the Provost and I had discussed the need for such a privacy policy over a year ago, after an incident of e-mail access at Harvard University attracted considerable media notice, and a draft of that policy was actually in hand at the time the events surrounding the fraud investigation became public, causing considerable concern. As incidents at Harvard and other institutions have recently shown, AUB is by no means alone in the challenges universities face in dealing with the rapid development of technology and the need to balance privacy with institutional imperatives through established policies.

As to some specifics in the report of the Working Group:

1. The work of the Group has made clear that documentation and procedural protocols can be greatly improved. Since there was a dearth of explicit guidance

on that count last year, I want to reassure the community that the University Auditor was raising privacy issues and the privacy framework with me continuously, as I had to consider and balance various interests in authorizing e-mail access in the specific context of a fraud investigation, as per the University's standing Fraud Policy. The Chairman of the Board of Trustees and the Chair of the Audit Committee of the Board were also kept apprised of the unfolding investigation. Nonetheless, the challenge of making judgments on a day-to-day basis was exacerbated by the lack of a robust policy environment assigning clear responsibilities to personnel engaged in the task of investigation on the one hand and designed to protect individual privacy and institutional integrity on the other.

2. I also wish to reassure the community that no e-mail access occurred other than in the context of an approved investigation, and then with specific authorization.

3. I appreciate the Working Group's specific conclusion that "IA did not approach IT to find a technical solution to extract the specific mailboxes within the Data Center" and that there was no need to remove sensitive e-mail data from the IT Data Center in Van Dyck Hall. While the University Auditor fully concurs that physically removing the data was not an optimal solution, his consultations with IT technical staff persuaded him that the environment of the Data Center was not designed to enable both the targeted access and the confidentiality of the whistleblowers. Given the need to achieve both objectives, I continue to see his decision to relocate the encrypted data as a difficult call to make, but reasonable under the circumstances.

4. We are all in agreement that improvements in the IT environment going forward will greatly assist those responsible for performing authorized investigative work to do so in an environment that is appropriately framed to balance critical privacy and institutional integrity principles.

5. I note that multiple policies exist to govern our individual obligations and responsibilities for the security, confidentiality, and privacy of our data and collections of records. Importantly, the Working Group has helped us see a need to improve the harmony of these policies and procedures. The lack of harmony among policies can make it difficult for employees to be aware of their responsibilities, and broad education among all members of our community regarding privacy, institutional needs, and policy and procedural compliance remains a pressing need.

Once again, I wish to thank the faculty members who generously gave their time to assess our policies and procedures regarding IT security and privacy. I also appreciate the time spent by members of the administration who met with the Group to clarify the events surrounding the incident. We have learned much from the endeavors and recommendations of the Group, and on the basis of their work we are committed to improving our security and privacy environment in the interests of academic freedom and institutional needs.

President Peter Dorman
February 24, 2014

Report of the Faculty Working Group on IT Data Privacy

January 22, 2014

Introduction

On May 14, 2013, President Peter Dorman formed a working group of faculty members (Faculty Working Group – FWG) to "review the protocols, policies, and procedures of the university's Information Technology organization as they relate to the protection of e-mail database and archive integrity, including encryption, chain of custody and related matters. Additionally, the Group will review the university's current technical environment as it relates to the need to protect the privacy of data while conducting highly targeted confidential access to the university's e-mail database and archives by authorized individuals granted such access by the President, and will recommend such measures as may be appropriate to ensure the integrity and security of the university community's confidential data." (Email message of President Dorman to the members of the FWG and others, dated May 26, 2013).

The FWG was convened soon after questions about email data privacy and security were publically raised (e.g. during the Senate meeting of April 26, 2013) by AUB faculty members who had learned that the Internal Audit (IA) Office had obtained copies of the contents of faculty and staff email accounts on portable hard drives, and that these accounts could be accessed by the IA staff outside the confines of the IT Data Center.

The FWG membership consisted of: Mazen Al-Ghoul (Professor, FAS), Zaher Dawy (Associate Professor, FEA), Imad Elhajj (Associate Professor, FEA), Ayman Kayssi (Professor, FEA; FWG Chair), and Alan Shihadeh (Professor, FEA).

Methods

The working group reviewed the following documents: a draft policy on data privacy from the Office of the Provost (dated March 26, 2013), the current charter of the Office of Internal Audit (last updated May 13, 2013), the previous charter of the Office of Internal Audit (last updated March 12, 2010), AUBnet (email) Accounts Policy (August 4, 2003), AUB Data Security Policy (AUB-IT-000005, October 2012), AUB Access Control Policy (AUB-IT-000035, December 2012), as well as other draft, under-preparation, internal IT policies and

procedures documents provided by the Chief Information Security Officer (CISO).

In addition to available documents, the working group used the recent instance involving the copying and transferring of email data as a case study to review the processes by which data privacy and security are protected at AUB, including the relevant decision hierarchy. To do so, the working group began by identifying key individuals from the AUB organization chart who are connected to data security and privacy and interviewed them. Ten interviews were conducted, totaling more than 15 hours of discussion during June 2013. The individuals who were interviewed were: President Peter Dorman, Provost Ahmad Dallal, COO George DeBin, then-CIO Rita Khayat, VP-Legal Affairs Peter May, University Auditor Andrew Cartwright, then-Associate CIO Joe Hage, CISO Ghassan Hitti, Interim Manager - IT Systems and Storage Samih Ajrouch, and Manager of IT Telecom Rima Assi. With the permission of the interviewees, all meetings except two (the meeting with VP-Legal Affairs and the meeting with the University Auditor) were audio-recorded.

Although the FWG met with the University Auditor, the request by the group to meet with the IT Audit Managers at the IA Office was denied. The FWG was also denied access to what it deemed to be relevant documents that were in the possession of the IA Office and the VP-Legal Affairs.

After a thorough analysis of the contents of documents, interviews, and meetings, a verbal report was presented by the FWG to President Dorman and Provost Dallal in a meeting that took place on June 18. The FWG also met with the President and the Provost on July 31, October 4, and October 26, 2013, and on January 22, 2014.

Key Findings

A. General

1. There is currently no policy at AUB that deals explicitly with data privacy.
2. Although the AUB Code of Conduct for Users of Computing Systems and Internet Services mentions that the "University reserves the right to conduct a full audit that may include an inspection of the contents of the subject's user files", there is currently no policy at AUB that deals explicitly with access to email-boxes by non-owners.
3. Email records are considered property of AUB; they can be accessed when deemed necessary by the IA and when such access is approved by the President.
4. In the context of authorization and data access, serious administrative decisions were made verbally with no official written communication.
5. Communication channels among IA, IT, and the upper administration (President, Provost, Vice Presidents) were lacking in certain critical instances, which led to inaccurate information propagation and impeded decision-making.

B. Information Technology Organization

1. The existing security procedures for log and event management of email and telecom systems are not adequate.
2. The existing security procedures for accessing information archives for investigative purposes are not adequate (chain of custody of physical disks, password protocols, access to data outside data center, destruction of copies, etc.)
3. There have been efforts since the end of 2012 to revise and upgrade policies and procedures related to information and IT security; these efforts are mainly led by the CISO.
4. There is lack of clarity in terms of the division of roles and responsibilities related to information security regulation and implementation between IT and CISO.

C. Internal Audit

1. In accordance with its charter, the IA Office has wide-reaching powers, which include authority to access all University documents or communications, whether print or electronic, and under necessary circumstances without prior notification of parties involved. These powers were exercised without a clear mechanism for oversight during the audit investigation.
2. Constructive and open communication between IA and IT was obstructed by an apparent mutual lack of trust between the two offices.
3. Since January 2012, the IA Office has regularly received phone logs of all outgoing and incoming calls to AUB campus extensions (excluding campus housing).

D. Recent Incident of Copying and Transferring the AUB Email Database outside IT Data Center

1. The events took place within the timeframe April 4 to April 19, 2013.
2. Prior to the email database incident of April 2013, copies of email log files (containing communication patterns, without the full email data) were provided in encrypted format by IT to IA to be given to VP-Legal Affairs.
3. Also prior to the email database incident, IA was intending to mirror the complete email system of AUB in order to obtain immediate real-time access to mailboxes. Real-time access was also requested to the telephone logs.
4. In the context of a time-sensitive investigation whereby confidentiality is critical, IA needed to access a specific mailbox from a specific period of time. Because the needed mailbox data was stored on an encrypted archival tape, it was not readily accessible.
5. Since the format in which the data stored on tape did not allow for targeted retrieval of a specific mailbox, the entire email database was restored to a hard disk within an encrypted container. The total size of the retrieved email data was more than 3 Terabytes. The data was copied in duplicate on two external hard disks, and re-encrypted with new passwords.
6. The data on each disk was encrypted with a two-part password. One half of the password was with a staff member in IT and two staff members in IA,

while the other half was with another staff member in IA and VP-Legal Affairs.

7. Mailboxes of all faculty and staff users on Microsoft Exchange were retrieved from the backup tapes of December 2012 and January 2013 directly onto the encrypted disks. The request was initiated by IA on April 4 and the copying was completed by IT on April 10.
8. In an email to the upper administration on April 11, CISO questioned the appropriateness of removing the email archive on disk from the IT Data Center.
9. Asserting that IT did not possess the needed software tool to extract specific mailboxes from the disks in a form that would allow the establishment of an audit trail, IA took possession of the disks and moved them to the IA office.
10. IA did not approach IT to find a technical solution to extract the specific mailboxes within the Data Center instead of copying all mailboxes on hard disks and moving them to the IA office outside the IT Data Center premises.
11. CISO was instructed to comply and provide the two hard disks to the IA; the handover took place on April 16 in the evening.
12. A protocol was developed between CISO and IA before the handover took place on April 16; however, there was at least one item in the protocol that was not implemented as agreed. The FWG was not able to verify the level of implementation of the protocol since IA did not share the protocol document.
13. IA reported that the two disks were in its custody for three days. The disks were placed in a safe inside the IA office. The two audit managers involved in the investigation had access to the safe.
14. Two disks were destroyed in the presence of IA staff only, on the evening of April 19. CISO and an IT staff member were invited to attend, but did not find it necessary to do so because the disks had no verifiable chain of custody, and could not confirm that the disks being destroyed were the original and only copies of the database.
15. The disks serial numbers were not documented by IT and the data on disks was not hashed to guarantee integrity of data, due to lack of time.
16. VP-Legal Affairs was provided a legal opinion that IA's access to all mailboxes was in-line with existing Lebanese laws.

Conclusions and Recommendations

1. There is a severe lack of privacy-related knowledge, policies, and procedures, and an absence of integrity-preserved logging and alerting mechanisms.
    - Recommendation: Develop policies and procedures to protect the privacy of data for members of the AUB community, including hardening of associated logs. These policies should also require that persons under investigation be notified within a defined period if their data was accessed, and should require that faculty and staff users of AUB IT systems be made aware that their data may be accessed by authorized university officials. Such authorization should stem from a committee charged with this duty.
2. Regarding data security and privacy, communication between IA, IT, and the upper administration lacks clarity, timeliness, and documentation.
    - Recommendation: A protocol should be developed to ensure efficient, well-documented communication.
3. The mailbox data needed for the IA investigation could have been retrieved from disks within the IT Data Center premises while maintaining confidentiality. There appears to have been no valid reason for IA to remove the disks from the Data Center.
    - Recommendation: A policy should be developed which disallows removal of data from the IT Data Center without specific justification and authorization.