

Draft Notes, Labor/Management meeting, Thursday, November 10, 2005

Present: Jim Dix, Fran Goldman, Dennis Selzner, Darryl Wood, Joe Schultz, Shelia Doyle

1. *Preliminaries.* UUP mentioned that Beth Kilmarx was unable to attend the meeting because of an undercurrent of pressure from management implying that she was spending too much time on union activities. UUP requested management not act at this point.

UUP discussed a new two-step approach to Labor/Management meetings: 1. discussion and agreement on an issue or problem; and 2. exploration of ways to address the issue or solve the problem. UUP recognized that Management is charged with solving problems brought up at L/M meetings, and that Management would give regular updates to UUP on progress toward solution of problems. Both UUP and Management agreed on this new approach to L/M meetings.

2. *Use of Social Security Numbers.* Problem raised by UUP: indiscriminate use of SSNs by various campus entities increases unnecessarily the chance of identity theft. Management agreed that this was an issue, and discussed steps they have taken to decrease the use of SSNs. These included two memos sent to faculty and staff (see attached); removal of SSNS from the database and signups forms at FitSpace; removal by Mark Reed, Director of Computing Services, of SSNs from many forms; placement of SSNs security on the agenda of the Enterprise-Wide Data Committee. Management also stated that SUNY Central and Payroll were exploring an identification system that did not require SSNs. UUP mentioned that faculty class lists still contain instructor's SSN, and brought up other instances in which SSNs were not necessary; UUP will provide Management with more details on these other instances.
3. *Campus evacuation plan.* Problem raised by UUP: there is a lack of information about BU's evacuation plan in the event of, for example, a terrorist incident. Management responded that according to Bill Dunn, Assistant Chief of Police, this information is secret because such information could be used by a terrorist in inflicting more damage. UUP stated that UUP members wish to be reassured that such a plan exists. Management said it would bring up the issue at the December-January meeting of the Disaster Planning Committee. UUP stated that at the least, the assurance that a notification plan in the event of a campus-wide emergency existed should be promulgated to the campus community.
4. *Annual distribution of Appendix 30 information to part-time employees.* Problem raised by UUP: the provisions of Appendix 30 of the UUP-State contract are not being disseminated to people who need to know them. Article 30 of the contract states that "The University shall instruct campuses to appoint part-time term faculty to full year appointments where they are in a position to do so."; "The University shall encourage campuses to provide support services and facilities needed by part-time faculty in conjunction with the performance of their professional obligation"; and "The University shall instruct each campus to publish whatever hiring procedures it has in place for filling part-time faculty vacancies." Management stated that it would include chairs in their boiler plate memo regarding Appendix 30 matters, and UUP stated that it would disseminate the information to part-timers.

5. *Visits by FBI or other law enforcement personnel.* Problem raised by UUP: UUP members are disconcerted when FBI agents show up unannounced at member's office door requesting interviews. Management stated that FBI agents coordinate with Barb Westbrook, University Counsel, for their visits on campus. UUP requested that the University Counsel's office notify the member before the FBI shows up at the member's door. Management replied that that is the formal policy of BU. Recently, a new FBI agent has been assigned to the area and that the agent was not familiar with BU/FBI protocol. Management stated that it would incorporate the formal notification of a member into management procedures for outside contacts in personnel matters. UUP suggested that the FBI agent be provided an authorization form from the University Counsel's office to show a member that the visit had been vetted through channels. Management agreed that this was a good idea.
6. *Sodexo, the BUCS card, and other potential contracting out.* Potential problem raised by UUP: the use of cards such as the BUCS cards could lead to contracting out of work done by UUP, resulting in fewer UUP jobs. Example: there was a person in the library that used to collect fines; now Sodexo can collect fines, eliminating the need for a fine-collection person. This not now a problem (the fine collecting person was CSEA, and moved to another job at the library), but could be one. Management stated that they had no plans that would amount to contracting out of work performed by UUP members.
7. *Discretionary salary increase hold-backs.* Problem raised by UUP: there is a lack of information about the specifics by which DSI money flowed from the president on down to the departments. Management referred to an email message from Sylvia Hall, Director of Human Resources (see below). UUP stated that it had requested a dollar amount or percentage of that was retained at each level, and criteria by which the retained money was allocated. Management said that it would not provide that data, that their final answer was provided in Hall's memo, and that UUP or concerned members should approach the VPs, Deans, and Chairs to obtain the information.
8. *One-year appointments of professionals after two years of full-time service.* Problem raised by UUP: professionals who have been here two or more years and do not have permanent appointment are given one-year renewal appointments when multi-year renewals are more appropriate. Management agreed with UUP that this was a problem. However, Management sees the HR office as advisory only. While they recommend when asked that renewal appointments be for two years, they do not enforce the recommendation.
9. *Employee organizational leave.* Problem raised by Management: notification of employee organizational leave is often post facto, instead of "reasonable advance notice" as per contract. (Employee organizational leave (EOL) is allowed in Article 11 of the contract to attend, for example, UUP Delegate Assemblies or grievance meetings.) HR often does not know EOL has been taken when HR is contacted by supervisors. Management suggested that employees requesting EOL email HR directly.

Memorandum

August 31, 2005

From: Mark Reed, Associate VP for Computing

To: All Faculty and Staff

Re: Threats to Data on Networked PCs and Via Printouts

Recent news and current public service advertising have alerted us all to the dangers of identity theft. Personal identity information has clearly become a target for hackers. I am writing to remind faculty and staff of the danger of storing sensitive, personal information about other people on networked PC's, and the importance of handling printouts of such information with care.

Many of us have a legitimate need to use such information in the performance of our duties, but we must remember that protecting it is both a legal and ethical obligation. In today's networked environment, attempts at hacking and intrusion of networked machines are common, and even machines that are up-to-date on software patches and have current anti-virus software can be hacked. No one at the University should be storing confidential information on a networked PC that is not specially protected; doing so is asking for trouble. Printing such information and failing to protect it while in use and/or improperly disposing of it afterwards is likewise risky behavior.

The University's standing Enterprise Data Committee has established guidelines for use and release of university data (see <<http://computing.binghamton.edu/policies/enterprisedata.html>>). The guidelines identify which data is considered confidential, provide reasonable justification for internal use and list restrictions concerning potential release of such data. Every department should be familiar with these guidelines. In general, personal information about individuals that is not "directory" information must be treated as confidential.

We can all work toward the better protection of data in the workplace. If there is no requirement that data on a PC be on the network, then the PC should be isolated from the network. If network access is required, then an acceptable approach is to allow access by PC, but store the information at a specially-protected source like a server. Making copies (or unnecessary printouts) of data files of sensitive information should be avoided, as duplication increases the chances for inadvertent disclosure. If copies must be made and placed on networked PC's, unauthorized access may be made more difficult by creating firewalls to limit and control access to the machine, or using encryption and writing sensitive data to removable media like thumb drives or CD-ROM's which are kept off-line when not in use. Likewise, printouts of sensitive information should be protected while in use and destroyed when no longer needed.

If you currently store confidential or sensitive information on a networked PC or laptop, or print it, you should immediately review the need to do so. Please consider the potential for outside or unauthorized access and take positive steps to protect the data. Computing Services can help

assess your situation and recommend steps to protect confidential information. Feel free to call your regular contact here or call Dick McCarthy (7-6106), Mike Hizny (7-4739), Jim Wolf (7-6194), Frank Saraceno (72015) or me (7-6112) if you would like to discuss this or need further information.

cc: Jim Van Voorst, Vice President for Administration

=====
Original Message-----

From: Binghamton University Faculty and Staff

[mailto:FACULTYSTAFF@LISTSERV.BINGHAMTON.EDU]On Behalf Of Gordineer,

Rhonda

Sent: Monday, September 12, 2005 11:33 AM

To: FACULTYSTAFF@LISTSERV.BINGHAMTON.EDU

Subject: Message from Mark Reed

All Faculty and Staff:

This email is a follow-up to my memo to you dated August 31st. Please take the time TODAY to check any networked device, web server, or publicly-accessible machine under your control for any information, whether in test or production form, that contains sensitive data, especially personally-identifying information about students or colleagues. If such information does not need to be there, remove it. If it has to be there, then review the security arrangements you have made and make sure they are adequate (see below if you're not sure how). Taking such actions now will help avoid the serious consequences later of inadvertently compromising sensitive information about students, faculty and staff, or dealing with the erosion of public confidence and reputation that follows a breach of security. It will also save you and your department from being in the position of having to apologize to colleagues or students for any action - or lack of action - that could cause them significant inconvenience or financial difficulty in this era of identity theft.

As a result of questions received in response to the 8/31 memo, we have posted a web page listing good practices and frequently-asked-questions about this topic at <<<http://computing.binghamton.edu/policies/datasecurity.html>>>. We'll add to it as we receive further questions and suggestions. I hope this list will prove to be a good resource for the campus on this topic. Per the 8/31 memo, if you need clarification on the University's data-use guidelines, please refer to <<<http://computing.binghamton.edu/policies/enterprisedata.html>>>.

Thanks for your help and attention!

-Mark Reed

Associate VP for Computing & Educational Technology

=====
From: Hall, Sylvia

Sent: Friday, October 28, 2005 12:02 PM

To: Wood, Darryl

Cc: Joe Schultz (jschultz@binghamton.edu)

Subject: Question on discretionary

Hi Darryl. I'm sorry that it took me a bit to get back to you re: your question on discretionary funds and how they are dispersed to the deans and others as awards for UUP represented employees are considered. In a follow up conversation you shared with me that your real focus was on academic departments, where you had received questions from some of the chairs re: the dollar amount they were given to distribute.

Here is what I can report:

- As indicated the President does ask that a small dollar amount be kept aside for her use in augmenting awards. It is not a percentage and has varied over the years, but generally is around \$15K

- The only VP that I know of who keeps additional funds for his/her use is the Provost and it is my understanding that she generally uses to recognize promotions. Apparently there is a mandatory \$1,000 for academic promotions that the Provost provides and often schools supplement that from their funds as they see fit.

- As for what arrives in Dean's offices for their use, after setting aside what she needs for the above-noted purpose, the Provost's office staff divides the funding up in a pro-rata form based on numbers of eligible UUP employees in each area.

- At this point, practices differ based on the individual Dean's practice and preference. In both cases where you raised a question – Harpur and Watson – the Dean keeps money aside for his use in further supplementing promotions, recognizing excellence awards, provide discretionary awards to department chairpersons, fund the alternative process (requests that come forward to the dean in other-than-the usual way), etc.

I hope this is helpful to you – it represents the very best I could do to pull together information as you had requested.

Thanks and have a good weekend.