Computer Science Department IT Policies and Procedures

The Computer Science (CS) Department abides by all policies, standards and procedures put forth by the President's Office, the University of Massachusetts, and the Information Technology Services Division (ITSD), the University of Massachusetts Boston. A detailed list of the university IT policies and procedures is posted on http://www.umb.edu/it/policies/ and http://www.massachusetts.edu/policy/datacomputingpolicies.html.

In addition, the CS Department Lab Policy is posted in http://www.cs.umb.edu/sp/about/facilities/policies/. The CS Department IT policies and procedures are stated as follows:

1. **System wide policy/procedure communication**

   The CS department will distribute new policies and procedures to its faculty and staff members for review. After discussions and modifications, the policies and procedures will be posted on the department website www.cs.umb.edu. These policies and procedures will be reviewed and updated as needed.

2. **Operating system patching/upgrading procedures**

   For the department's Windows PCs, patching to the operating system will be done automatically using the auto update procedure provided by the operating system. For non-Windows PCs and servers, patching will be applied on an as-needed basis. To accommodate the needs of our faculty and staff in teaching, research and Lab maintenance, operating systems need to be upgraded from time to time. This will be applied on an as-needed basis.

   Patching/upgrading of the operating system will be handled in the manner as stated in the Application Development and Change Control procedures.

3. **Data inventories**

   On a periodic basis, the CS Department will conduct an inventory of data that is stored in both hard copies and electronic media. We will categorize the data into Confidential, Operational Use only, or Unclassified based on the different document types. To ensure that the sensitive data elements get protected, we will follow appropriate security precautions to protect vital records

as stated in the University of Massachusetts Records Management, Retention and Disposition Standards.

After the data elements have been inventoried and categorized, their disposal will follow the department retention schedule as shown:

Document Type	Security Classification	Security Precautions	Shred Date
Personnel Action Form (Student)	Confidential	In binders in locked/occupied admin office	After graduation
Personnel Action Form (Faculty)	Operational Use Only	In binders in locked/occupied admin office	None
Academic Scheduling files	Unclassified	Locked filing cabinet	10 years
Degree Audits	Confidential	Locked filing cabinet	10 years
Student Time Sheets	Unclassified	In binders in locked/occupied admin office	5 years
Staff Time Sheets	Unclassified	In binders in locked/occupied admin office	5 years
Graduate Student Applications	Confidential	locked filing cabinet	2 years
Grad Student Files	Confidential	Locked filing cabinet	10 years
Teacher Evaluation Bubble Sheets	Unclassified	Locked filing cabinet	3 years
Teacher Evaluation Comment Sheets	Operational Use Only	Locked filing cabinet	5 years after instructor leaves
Final Grades	Confidential	Locked filing cabinet	Never
Graduate Student Appointment Forms	Operational Use Only	In binders in locked/occupied admin office	10 years

Vendor Add/Update Forms	Confidential	Locked filing cabinet	2 years
Reimbursement Documentation	Confidential	Locked filing cabinet	6 months
Pre-Employment Paperwork	Confidential	Locked filing cabinet	6 months

4. Asset Inventories

Assets owned by the CS Department are listed in an Excel spreadsheet and maintained by the Department Property Custodian. Items tagged as surplus or transferred to another department remain on this list and are noted as surplus or as transferred to a specific department with the date recorded. As new assets are acquired, they are added to the list.

Given the small number of assets maintained by the CS Department, the asset list is compared with the university's Asset Management System (AMS) inventory for CS twice a year to uncover any possible conflicts or omissions. Working with the University Property Manager, the Department Property Custodian rectifies the discrepancies between the department spreadsheet and the inventory shown in AMS.

5. Disposal of IT equipment

All IT and moveable equipment are disposed of in accordance with the University of Massachusetts Boston's Inventory Control Policy & Procedure for Moveable Equipment (policy number FY10-PRO-001-00), issued March 30, 2010 by the Administration and Finance Department.

Once items are identified as surplus, the Department Property Custodian contacts University Customer Service and creates a work ticket. The custodian completes the appropriate forms in accordance with the above policy, acquires the CS Department Chairperson's signature, and schedules the surplus for pickup and disposal. All surplus items are then noted as such in the department's asset inventory spreadsheet as well as that in the AMS.

6. System Access for New Hires/Transfers/Terminations

In the case of a new hire/transfer/termination, the CS Department Chairperson or the responsible faculty member will initiate a request for the corresponding system access action. This may include adding or deleting the user's access to department facilities, mailing lists, computer systems, and department managed applications. The initiation and the subsequent resolution of the request will be tracked using the Operator Request Queue.

7. User Access Reviews

The CS department will conduct user access reviews on all PCs and servers on a yearly basis. Owners of PCs and servers will be notified of the review by emails from operator@cs.umb.edu. They will check users' access to their computers against their responsibilities. Users whose responsibilities do not require access to the equipment will be deleted. For PCs and servers administered by the department, the reviews will be conducted by the CS Department System Staff. Progress of these reviews will be documented in the Operator Request Queue.

For critical CS department managed applications, the list of users with administrator or staff access will be compiled and reviewed with our clients once a year. Users whose responsibilities do not require access to the applications will be deleted. Progress of these reviews will be documented in the Operator Request Queue.

8. Incident Handling and Escalation

All notices of security incidents from system monitors, users, student operators, and complaints from campus IT or the Internet will be directed to operator@cs.umb.edu. For urgent matters, they will be reported to the CS Department System Staff at 1-617-287 6480. A ticket at the Operator Request Queue will be generated to track its progress.

After evaluating the scope of the incident, the CS System staff will prioritize the security incident. Depending on its severity, the staff may escalate the incident and notify the CS Department Chairperson and/or the university's security department.

The CS System Staff will take immediate action, if necessary, to mitigate an urgent situation. Such action may include disabling rogue accounts or taking compromised hosts off the network. After the remedial action, the security incident initiator will be notified and he has to verify that the incident has been resolved. Progress of the incident handling will be tracked using the Operator Request Queue and archived for later analysis.

9. Application Development and Change Control Procedures

For user requests logged in the Operator Request Queue that may impact the IT operations of the CS Department, they will be reviewed by the CS Department Change Control Committee comprised of the CS System Staff, the CS Lab Director and/or the Department Chairperson. Examples of these requests include Operating systems upgrade and patching. They may be denied or approved based on technical, resources limitations or business reasons. Communications of the decision to the requestor will be done via email. For those approved requests, the requestor will have to verify the changes after their implementations. Progress of these requests will be tracked in the Operator Request Queue.