



Office of the Mayor
City of Columbus
Ohio

EXECUTIVE ORDER

2007- 03

Michael B. Coleman, Mayor

September 25, 2007

WHEREAS, the City of Columbus stores and maintains sensitive information within its computer systems, and if not properly safeguarded, this sensitive information can be compromised placing the City, its employees and citizens at risk; and

WHEREAS, sensitive information shall include, but not be limited to, social security numbers, health information, and credit card information, past, present and future; and

WHEREAS, all City employees, students and interns, must safeguard all sensitive information, City-owned computer systems and computer equipment from being lost, stolen or compromised in any manner; and

WHEREAS, all City employees, students and interns, shall not download or copy sensitive information to any electronic devices to include, but not limited to, laptops, desktops, Blackberry's, PDA's, jump drives, etc.; and

WHEREAS, all City employees, students and interns, shall not print and/or remove sensitive information from City premises without proper authorization; and

WHEREAS, all City employees, students and interns must adhere to existing *Central Work Rules* and the *Comprehensive Electronic Communications Policy*; and

NOW, THEREFORE, I, Michael B. Coleman, Mayor of the City of Columbus, declare and institute this Executive Order outlining the policies in the proper handling of sensitive data; the steps taken if that data, or computer related equipment is lost or stolen, and disciplinary action for stealing and/or removing sensitive data without proper authorization; all City employees, students and interns are to follow:

A. PROPER HANDLING OF SENSITIVE DATA

All City employees, students and interns must comply with the provisions within the City of Columbus' Central Work Rules and Comprehensive Electronic Communications Policy (CECP) which set forth the proper handling of City equipment and sensitive data.

All city employees, students and interns must ensure prudent care and security is provided to any City property (i.e. laptops, PDA, Cell phones, Blackberry) to guarantee the security of this equipment and the information that is stored upon it.

September 25, 2007

Department management must ensure that proper administrative controls are in place to account for all copies or backup copies (i.e. tape media, jump/zip or floppy drives) of information that are stored offsite within alternate City locations or in commercial backup storage locations to which the City has contracted for this service.

Department management is responsible for reviewing data that is published for use on the City's Intranet or Internet to ensure that sensitive information is not being placed upon internal or external websites.

Any questions concerning the security of sensitive data or information shall be directed to the Department of Technology for review, guidance and disposition.

B. STEPS TO TAKE IF SENSITIVE INFORMATION OR EQUIPMENT IS LOST OR STOLEN

Should a PC, laptop, jump-drive or any other equipment that contains sensitive information be lost or stolen, the employee discovering the loss must immediately:

- Contact the DoT Help Desk (645-5758) to report the loss and initiate recovery system protection actions.
- Report the loss up through the departmental chain of command indicating the potential sensitivity of the data that is on the equipment.
- Contact the Columbus Police Division (CPD) to notify them of the loss. Individuals must communicate the potential sensitivity of the lost data and cooperate fully with the CPD investigation in an attempt to recover the equipment/data.

The department which has lost the sensitive information or equipment shall cooperate fully with DoT in an attempt to minimize the exposure of the City of Columbus by providing all information necessary to mitigate the risk imposed by the loss. DoT will act promptly deactivating accounts and network access.

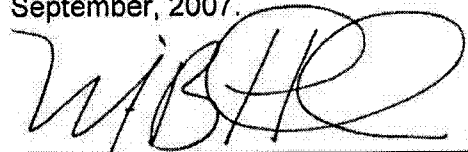
C. DISCIPLINARY ACTION

Any City employee, student or intern who does not adhere to the City's Central Work Rules or Comprehensive Electronics Communications Policy is subject to disciplinary action.

Any exceptions to this Executive Order must be requested in writing and approved by the Mayor, Department of Technology and the Department of Human Resources.

This order shall be in full force and effect after my signature is affixed to this document.

IN WITNESS WHEREOF, I have hereunto set my hand and caused the Great Seal of the Mayor of the City of Columbus, Ohio to be hereto affixed this 25th day of September, 2007.



Michael B. Coleman
Mayor

September 25, 2007