Summary of the Practical Impact of the Written Information Security Program for Non-Public Documents

The Written Information Security Program (WISP) sets forth rules to prevent disclosure of **non-public documents** containing personal information held by the Massachusetts courts. **The definition of personal information in this WISP does not include information that is lawfully available to the public from federal, state or local government records.** More specifically, for the purposes of this WISP, **personal information does not include information that is contained in case files that are publicly available**.

Personal information not publicly available by law or court rule may be contained in Juvenile Court records, Probate and Family Court records, the records of the Office of the Commissioner of Probation, the Office of Jury Commissioner and other Trial Court departments. Virtually all Courts have impounded files and personnel files containing personal information. Those files are non-public and employees must prevent their disclosure to the public.

Each department of the Trial Court and each appellate court must have practices in place to prevent the disclosure of impounded and other non-public documents. Employees must know and understand their court's practices and consistently comply with them.

Employees must not leave personal information (in physical files or on computers) in the open where unauthorized individuals can access it.

Employees must not transport or store personal information outside the court where unauthorized individuals may access it unless the employee takes appropriate measures to ensure the security of the information. Employees must be conscious of the risks inherent in taking electronic records containing personal information off court premises. Any electronic records taken off court premises should be on a court-owned and password-protected device.

Physical access to records containing personal information should be restricted to those employees who need to see the personal information. Each court must ensure that personal information is not disclosed to anyone but the person to whom such disclosure is intended. For example, if personal information must be sent through the mail, employees must take reasonable steps to ensure that only the intended recipient receives the personal information, for example, by marking the envelope "confidential."

Employees should not leave messages containing personal information on voice mail systems.

Employees should not fax documents containing personal information without taking steps to ensure their confidentiality, *e.g.*, that the recipient is alerted to expect the fax and asked to retrieve it immediately.

Employees must immediately report to their manager any inappropriate disclosure or loss of records containing personal information, whether accidental or intentional.

When discarding or destroying records that are known to contain personal information, employees must redact, burn, pulverize or shred paper documents and destroy or erase electronic media.

WRITTEN INFORMATION SECURITY PROGRAM
FOR NON-PUBLIC DOCUMENTS ("WISP")

I. PROGRAM STATEMENT

This Written Information Security Program ("WISP") sets forth standards for the protection of **personal information in non-public documents** held by the Massachusetts courts. **The definition of personal information in this WISP does not include information that is lawfully available to the public from federal, state or local government records**. This means that, for purposes of this WISP, **personal information does not include information that is contained in case files that are publicly available**.

This WISP implements the provisions of the Supreme Judicial Court Order Re: Protection of Personal Information in the Judicial Branch dated January 7, 2010, which was issued pursuant to G. L. c. 93H, § 2(c). The WISP sets forth the standards applicable to the Supreme Judicial Court, the Appeals Court and all departments of the Trial Court ("Courts") for collecting, storing, using, transmitting, and protecting electronic and physical records containing personal information. For purposes of this WISP, "personal information" means a person's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to that person: (a) social security number; (b) driver's license number or state-issued identification card number; or (c) financial account number or debit or credit card number with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account.

II. PURPOSE

The purpose of the WISP is to: (a) ensure the security and confidentiality of personal information; (b) protect against any anticipated threats or hazards to the security or integrity of such information; (c) protect against unauthorized access to, or use of, such information in a manner that creates a substantial risk of identity theft or fraud.

III. SCOPE

In developing and implementing the WISP, the Courts have (1) considered reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information; (2) assessed the likelihood of occurrence and the potential damage resulting from these risks, taking into consideration the sensitivity of the personal information; (3) evaluated the sufficiency of existing policies, procedures, and other safeguards in place to control risks; and (4) designed safeguards to minimize those risks. The Courts will regularly monitor the effectiveness of those safeguards.

IV. WISP ADMINISTRATORS

The Executive Director of the Supreme Judicial Court, the Court Administrator of the Appeals Court and the Chief of Staff of the Administrative Office of the Trial Court, or their designees

(collectively, “WISP Administrators”) are responsible for the supervision, implementation, coordination and maintenance of the WISP.

V. COLLECTION AND STORAGE OF PERSONAL INFORMATION:

To perform their judicial functions, the Courts must collect and store personal information. For example, the Courts collect and store information from employees, job applicants, vendors, parties, witnesses, jurors and victims. Personal information not publicly available by law or court rule may be contained in Juvenile Court records, Probate and Family Court records, the records of the Office of the Commissioner of Probation, the Office of Jury Commissioner and other Trial Court departments. Personal information may also be contained in impounded files and personnel files.

The amount of personal information collected by the Courts should be limited to the amount reasonably necessary to accomplish the Courts' business. To address risks to the security, confidentiality and integrity of personal information, the following measures shall be taken:

a) Courts will inform employees that personal information must be kept secure and disclosed only in accordance with the law and applicable court rules.

b) To the extent reasonably feasible, the Courts will not collect personal information through e-mail.

c) The Courts will control access to records containing personal information. Physical access to records containing personal information should be restricted to those who need to see the personal information. Court employees should handle personal information discreetly and guard against unauthorized access to records containing personal information.

d) The Courts will not store electronic records containing personal information on computers, storage media, or electronic devices that are not secured against unauthorized access. Any Court records containing personal information that are taken off court premises should be on a court-owned and password-protected device. Employees should be mindful of the risks inherent in taking electronic records containing personal information off court premises and in transferring information from court-owned to employee-owned computers and storage media, and should minimize such transportation, transfer and storage.

e) Upon separation from employment, an employee’s supervisor or an appropriate member of the employer court’s Human Resources Department will ensure that the departing employee does not have access to physical or electronic records containing personal information as follows: Terminated employees must return all records containing personal information in any form, and surrender all keys, IDs, access codes or badges that permit access to the premises or to personal information. Remote electronic access to personal information must be disabled. Voicemail access, email access and passwords must be invalidated.

VI. USE AND DISCLOSURE OF PERSONAL INFORMATION.

The Courts will use and disclose personal information in a way that allows them to perform their functions, but safeguards personal information from improper disclosure and to that end:

a) The Courts will take appropriate measures to ensure that personal information is not disclosed to anyone but the person to whom such disclosure is intended. For example, if personal information must be sent through the mail, the Courts will take reasonable steps to ensure that such personal information is received only by the recipient, for example, by marking envelopes "confidential."

b) The Courts should avoid transmitting records and files containing personal information across public networks unless it is done in a secure, encrypted way.

c) If personal information is improperly disclosed, the Courts will notify the appropriate Chief Justice as required by the Supreme Judicial Court Order of January 7, 2010.

VII. HANDLING OF PERSONAL INFORMATION.

The Courts will minimize the risks of inadvertent or unnecessary disclosure of personal information and to that end:

a) Courts will instruct employees not to leave personal information (in physical files or on computers or other electronic equipment having such personal information stored on it) in the open where it may be accessed by unauthorized individuals. Courts will further instruct employees not to transport or store personal information outside the office where it may be accessed by unauthorized individuals unless appropriate measures are taken to ensure the security of the information. For example, employees who take electronic files containing personal information off court premises should make reasonable efforts, including but not limited to speaking with their court's Chief Information Officer about technological resources available, to ensure that personal information being taken off court premises is secure.

b) Courts will instruct employees not to leave voice mail messages containing personal information on voice mail systems.

c) Courts will instruct employees not to fax documents containing personal information without taking measures to ensure their confidentiality, *e.g.*, that the recipient is alerted to expect the fax and asked to retrieve it immediately.

d) Courts will instruct employees to report to the designated manager in their court or department any inappropriate disclosure or loss of records containing personal information, whether accidental or intentional.

VIII. DESTRUCTION OF PERSONAL INFORMATION.

To the extent permitted by law and court rule and unless needed for a continuing purpose, the Courts will destroy records containing personal information. When discarding or destroying records in any medium that are known to contain personal information, the Courts must seek to comply with the minimum standards set forth in M.G.L. c. 93I for the proper disposal of records containing personal information, namely: (a) paper documents containing personal information should be either redacted, burned, pulverized, or shredded so that personal information cannot practicably be read or reconstructed; and (b) electronic media and other non-paper media containing personal information should be destroyed or erased so that personal information cannot practicably be read or reconstructed.

IX. THIRD-PARTY PROVIDERS.

The Courts will take all reasonable steps to verify that any third-party providing services to the Courts that has access to personal information has the capacity to protect such personal information in the manner provided for in this WISP. The Courts will take all reasonable steps to ensure that any such third-party service provider is applying protective security measures at least as stringent as those required to be applied to personal information under this WISP.

X. MONITORING.

Each WISP Administrator will regularly monitor the information security program to ensure that it is operating in a manner reasonably calculated to prevent unauthorized access to, or unauthorized use of, personal information. The Trial Court Information Services Department and the Information Technology departments of the appellate courts may make assessments of software use, conduct announced and unannounced audits of their respective Courts' computers, and take any other actions considered necessary to ensure compliance with this program. The Executive Director of the Supreme Judicial Court, all Court Administrators and Departmental Directors may make assessments of their respective employees' access to paper files containing personal information and will work with their employees to prevent unauthorized collection, storage, or disclosure of personal information.

XI. REVIEW OF PROGRAM.

The WISP Administrators will review and, where necessary, update the WISP at least annually or whenever there is a material change in personnel, governmental, technological, administrative or other practices that may appreciably undermine the efficacy of the program.

XII. REVIEW OF BREACH, RESPONSIVE ACTION, AND DOCUMENTATION OF RESPONSIVE ACTION.

If an incident of unauthorized access to physical or electronic records by an employee or third party has occurred, the WISP Administrator for the affected court will review the incident in a manner commensurate with the nature and scope of the unauthorized access to determine the possible breach of confidentiality, security, or integrity of the records, if any, and make any necessary changes in personnel, technological, or other practices relating to protection of personal information. The WISP Administrator for the affected court in his or her discretion (and consistently with any relevant collective bargaining agreements) may impose appropriate disciplinary measures for violations of the WISP. The WISP Administrator will document any action taken.

XIII. EMPLOYEE TRAINING.

The WISP Administrators will make efforts to integrate training on the WISP into the periodic training made available to court employees. WISP Administrators also will ensure that a copy of this WISP is distributed to each employee.

XIV. COMPUTER SYSTEM SECURITY REQUIREMENTS.

To the extent technically feasible, the Courts will use the following computer-related security measures:

a) Secure User Authentication Protocols. Control of user IDs and other identifiers; a secure method of assigning and selecting passwords consisting of at least seven letters and numbers; periodic password changes; control of data security passwords to ensure that such passwords are kept at a location separate from that of the data to which such passwords permit access; restricting access to active users and active user accounts, only; and blocking access to user identification after multiple unsuccessful attempts to gain access to the particular system.

b) Secure Access Control Measures. Assignment of a unique identification plus a password, which is not vendor-supplied, to each person with computer access. Requiring that Judicial Branch employees close their email accounts (Scalix, Outlook, Thunderbird, Modzilla) and log off their other user accounts (WordPerfect, Intranet, etc.) when leaving their computers unattended for a long period of time and, in any event, at the end of the work day.

c) Safeguards against Access by Former Employees. Ensuring that departing or former employees cannot access records containing personal information by terminating their physical and electronic access to such records, including deactivating their passwords and user names.

d) Protection of Personal Information Stored on Notebooks and Other Storage Media. Courts will instruct employees who download personal information to notebooks or other storage media to ensure that the data is password protected.

e) Monitoring. Reasonable monitoring of networks and systems to determine unauthorized access to, or use of, personal information and recording the audit trails for users, events, dates, times, and success or failure of login.

f) Firewalls. Installation of firewall protection with up-to-date patches, including operating system security patches. The firewall will, at a minimum, protect devices containing personal information from access by, or connections from, unauthorized users.

g) Antispyware. Installation of the most current version of system security agent software, which will include antispyware and antivirus software, including up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and which includes security software that is set to receive the most current security updates on a regular basis.

h) Education. Training and education of employees on the proper use of the computer security system and the importance of personal information security.

i) Network Security. Maintaining an appropriate level of security by permitting external access to the Courts' networks only with access to a Citrix account. The WISP Administrator and the Chief Information Officer of the respective Court must approve all Citrix access and any access to external networks from within the Courts' networks (this includes the use of PC Anywhere, GOToMyPC.com, MS Live, etc.) to connect to a home or otherwise external computer. Prohibiting the use of a modem in conjunction with network-connected equipment without prior written permission from the Chief Information Officer.

Posted: February 15, 2011