

940 CMR: OFFICE OF THE ATTORNEY GENERAL

940 CMR 27.00: SAFEGUARD OF PERSONAL INFORMATION

Section

27.01: Scope, Purpose, and Other General Provisions

27.02: Definitions

27.03: Written Information Security Program

27.04: Computer System Security Requirements

27.01: Scope, Purpose, and Other General Provisions

- (1) Applicability. 940 CMR 27.00 is applicable to the Office of the Attorney General (AGO).
- (2) Purpose. The Attorney General promulgates 940 CMR 27.00, relating to the Safeguard of Personal Information, pursuant to her authority in M.G.L. c. 93H, § 2(c).
- (3) The purpose of 940 CMR 27.00 is to effectuate the purpose of M.G.L. c. 93H, that is, to: ensure the security and confidentiality of consumer and employee information in a manner fully consistent with industry standards; to protect against anticipated threats or hazards to the security or integrity of such information; and to protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any resident of the commonwealth.
- (4) Scope. 940 CMR 27.00 governs the collection, maintenance, and disclosure of "personal information" as defined by M.G.L. c. 93H, § 1(a), and 940 CMR. 27.00.
- (5) Consistency. 940 CMR 27.00 should be read consistently with other state or federal laws and regulations applicable to the AGO and already in place, including but not limited to the public records laws (*e.g.*, M.G.L. c. 66, § 10; the Fair Information Practices Act, M.G.L. c. 66A, § 1; the Criminal Offender Record Information Act, M.G.L. c. 6, § 172; 940 CMR 11.00).
- (6) Limitation. 940 CMR 27.00 is not intended to establish a standard of care or create any independent private right, remedy, or cause of action on the part of any employee, consumer, or other third party on account of any action the AGO takes or fails to take in relation to the Written Information Security Program (WISP).

27.02: Definitions

For purposes of 940 CMR 27.00 and as used in 940 CMR 27.00, unless the context otherwise requires, the following terms shall have the following meanings:

Attorney General means the Office of the Attorney General (AGO).

Breach of Security means the unauthorized acquisition or unauthorized use of unencrypted data or encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

Computers means personal computers, laptops, and PDAs such as Blackberries.

Electronic means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

Encryption means the transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key.

27.02: continued

Personal Information means a Massachusetts resident'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 such resident:

- (a) Social Security number;
- (b) driver's license number or state-issued identification card number; or
- (c) financial account number, or credit or debit 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; provided, however, that "personal information" does not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Record or Records means any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

27.03: Written Information Security Program

The Attorney General shall develop, implement, maintain, and monitor a Written Information Security Program (WISP) designed to safeguard the personal information of residents of the commonwealth contained in the records of the Attorney General. The Attorney General's WISP shall be separate from 940 CMR 27.00 in order to facilitate periodic review and updating of the program. Like 940 CMR 27.00, the WISP shall be read consistently with the safeguards for protection of personal information of a similar character set forth in other state or federal laws and regulations applicable to the AGO and already in place, including but not limited to the Fair Information Practices Act, M.G.L. c. 66A, § 1; the Criminal Offender Record Information Act, M.G.L. c. 6, § 172, *et seq.*; and 940 CMR 11.00. The Attorney General's WISP shall be available for public inspection, except to the extent any section(s) thereof may be exempt from disclosure under M.G.L. c. 4, § 7, cl. 26, or are privileged by law.

The Attorney General's WISP shall include the following elements:

- (1) Designation of Employee. The Attorney General will designate one or more employees to design, implement, and coordinate the maintenance of the WISP.
- (2) Identification and Assessment of Internal and External Risks. The Attorney General will identify and assess internal and external risks to the security, confidentiality, or integrity of any electronic, paper, or other records containing personal information in each relevant area of activity of the Attorney General, and will evaluate and improve, where necessary, the effectiveness of the current safeguards for minimizing such risks, including but not limited to:
 - (a) ongoing employee training;
 - (b) monitoring employee compliance with policies and procedures;
 - (c) upgrading information systems, including network, system, and software design, as well as information processing, storage, and transmission, as necessary;
 - (d) storage of records and data in locked facilities, storage areas or containers;
 - (e) access and transportation of records and data by telecommuters and others who take records containing personal information off the AGO premises; and
 - (f) improving, as necessary, means for detecting, preventing, and responding to security breaches, including but not limited to security systems and failures.
- (3) The Attorney General will take reasonable steps to ensure that departing or former employees cannot physically or electronically access records containing personal information.
- (4) The Attorney General will take reasonable steps to verify that any third-party service provider with access to personal information has the capacity to protect such personal information in the manner provided for in 201 CMR 17.03; and will take all reasonable steps to ensure that such third party service provider is applying to such personal information protective security measures at least as stringent as those required to be applied to personal information under 201 CMR 17.03.

27.03: continued

(5) Collection of Information. The Attorney General will collect information required by law and the minimum amount of personal information reasonably necessary to accomplish the legitimate governmental purpose for which it was collected; will permit access to the smallest number of persons who are reasonably required to know such information in order to accomplish such governmental purpose; and will retain such information for the minimum time reasonably necessary to accomplish its purpose and consistent with laws and regulations governing public records retention.

(6) Access, Storage, Use, and Disclosure. The Attorney General will place reasonable restrictions upon physical access to records containing personal information including a written procedure that sets forth the manner in which physical and electronic access is restricted. The AGO will disclose the information only to those persons who and entities which reasonably require the information to perform their duties. The AGO will use and disclose the information only in conformance with a written procedure that sets forth the manner in which access to, and use and disclosure of such personal information is restricted.

(7) Monitoring. The Attorney General will conduct reasonable monitoring of systems to determine whether the WISP is operating in a manner reasonably calculated to prevent unauthorized access to or use of personal information and upgrading information safeguards as necessary to limit risks.

(8) Review of Program. The Attorney General 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 reasonably undermine the efficacy of the program.

(9) Review, Responsive Action, and Documentation of Responsive Action. Where the AGO learns that unauthorized access to physical or electronic records by a employee or third party has occurred, the AGO 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 to make any necessary changes in personnel, governmental, technological, administrative, or other practices relating to protection of personal information. The Attorney General in his or her discretion (and consistently with any relevant collective bargaining agreements) may impose appropriate disciplinary measures for violations of the WISP. The AGO will document any action taken.

(10) Destruction. The Attorney General will establish policies and procedures for the destruction of personal information as soon as it is no longer needed or required to be maintained by state or federal record retention requirements.

(11) Employee Training. The Attorney General will ensure that AGO employees are trained in the law and the AGO WISP relating to the proper collection, storage, use, and disclosure of personal information.

27.04: Computer System Security Requirements

With respect to information stored and maintained in electronic form, the Attorney General's WISP shall establish and maintain security measuring covering its computers, including wireless systems, that, at a minimum, and to the extent technically feasible, has the following elements:

(1) Secure user authentication protocols, including: control of user IDs and other identifiers; a reasonably secure method of assigning and selecting passwords consisting of at least seven letters and numbers; periodic changing of passwords; 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.

27.04: continued

- (2) Secure access control measures that restrict access to records containing personal information to those who reasonably need such information to perform their job duties, and assignment of a unique user ID plus a password, which is not vendor supplied, to each person with computer access.
- (3) Restricted access to computerized records containing personal information, including a written procedure that sets forth the manner in which access to personal information is restricted.
- (4) Safeguards Against Access by Former Employees. The Attorney General will ensure that departing or former employees cannot access electronic records containing personal information by terminating their electronic access to such records, including deactivating their passwords and user names.
- (5) Safeguards Against the Transmission of Personal Information. To the extent technically feasible, encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.
- (6) Reasonable periodic monitoring of networks and systems for unauthorized use of or access to personal information, and recording the audit trails for users, events, dates, times, and success or failure of login.
- (7) Encryption of personal information stored on laptops or other portable devices.
- (8) For electronic files containing personal information on a system that is connected to the Internet, 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.
- (9) The most current version of system security agent software which will include antispymware 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.
- (10) Education and training of employees on the proper use of the computer security system, the importance of personal information security, and resources available to safeguard personal information.
- (11) Enhanced Network Security.

REGULATORY AUTHORITY

940 CMR 27.00: M.G.L. c. 93H, § 2 (c).