MIIA
Nonprofit
Locally based
Member driven
Serving Massachusetts communities since 1982

GUIDELINES FOR RESPONDING TO IT PUBLIC RECORDS REQUESTS

Cybersecurity has become a Risk Management priority due to recent cyberattacks in both the public and private sectors. MIIA/MMA is working with the MassCyberCenter to provide you with tools to assist your municipality in this area. This memorandum provides you with information and guidelines for handling public records requests related to information technology and internal computer systems that may threaten your municipality's cybersecurity.

The Massachusetts Public Records Law grants persons a right of access to records maintained by governmental agencies and municipalities. G.L. c. 66, § 10; G.L. c. 4, § 7(26). Access includes the right to inspect and copy public records and/or obtain copies of such records (paper or electronic) upon payment of a reasonable fee. 950 CMR 32.07. Although the Public Records Law broadly defines "public records" to include "all books, papers, maps, photographs, recorded tapes, financial statements, statistical tabulations, or other documentary materials or data, regardless of physical form or characteristics, made or received by any officer or employee," it also contains several exemptions designed to protect from disclosure certain records that the Legislature has determined, for a variety of reasons, should not be considered "public."
G.L. c. 4, § 7(26)(a) – (v).

Recently, Massachusetts governmental agencies and municipalities have begun receiving public records requests for data and documentation relating to internal computer systems and information technology. For example, persons have requested records regarding firewalls, networks, switches, port counts, servers, remote access software, encryption software, secure user authentication protocols, and apps. Not surprisingly, such requests have raised legitimate concerns among agency and municipal IT departments that the sharing of internal IT data could facilitate unauthorized access to governmental computer systems, programs, and information and/or allow outside parties to encrypt governmental files with ransomware or other malware.

Those charged with the task of protecting cyber security on a local level should be aware that the Public Records Law contains safeguards that can be invoked in response to intrusive public records requests. Principal among those safeguards is Exemption (n) to the Public Records Law, which states in part that the following shall not be considered "public records":

> blueprints, plans, policies, procedures and schematic drawings, which relate to internal layout and structural elements, security measures, emergency preparedness, threat or vulnerability assessments, or any other records relating to the security or safety of persons or buildings, structures, facilities, utilities, transportation, *cyber security* or other infrastructure located within the commonwealth, the disclosure of which, in the reasonable judgment of the record custodian, subject to review by the supervisor of public records under subsection (c) of section 10 of chapter 66, is likely to jeopardize public safety or *cyber security*.

G.L. c. 4, § 7(26)(n) (emphasis added). Originally adopted in the wake of 9/11, the purpose of Exemption (n) was to assist governments in protecting the public from terrorist attacks by providing agency and municipal officials with the means of withholding certain records and information from public disclosure. To apply Exemption (n), Massachusetts courts have held that the records custodian (often an IT Director or Records Access Officer) must first determine whether the records sought resemble those expressly listed in the statute, such as plans, policies, and procedures relating to internal structural elements and/or security measures. Second, the custodian must exercise "reasonable judgment" to determine whether disclosure of the requested records "is likely to jeopardize public safety or cyber security." If he or she makes such a determination, the custodian may deny the public records request under Exemption (n).

In denying a public records request under Exemption (n), the custodian should provide the requesting party with sufficient facts to demonstrate to the Supervisor of Records or a reviewing court that a reasonable person would agree with the custodian's determination. For example, the custodian may conclude that the requested records provide a blueprint to a terrorist or hacker seeking to penetrate the municipality's data or network infrastructure. Or the custodian reasonably believes that disclosure of the requested records may compromise the municipality's ability to maintain confidentiality with respect to sensitive data, may jeopardize the municipality's ability to render essential government services and/or may expose the municipality to unknown financial or legal consequences. In the end, the custodian's determination will likely be upheld so long as it is "reasonable."

Given the nature of the data typically maintained by many governmental agencies and municipalities, local officials may also invoke Exemption (a) of the Public Records Law to withhold requested records under certain circumstances. Exemption (a) states that the disclosure requirements do not apply to records "specifically or by necessary implication exempted from disclosure by statute ." G.L. c. 4, § 7(26)(a). Without listing all of the many statutory exemptions, several examples include:

- Applicants for tax abatements or exemptions (G.L. c. 59, § 60);
- Participants in address confidentiality programs (G.L. c. 9A, § 6);
- Applicants for the termination of affordable housing restrictions (G.L. c. 40T, § 3);
- Birth certificates (G.L. c. 46, 4A);
- Records of the elderly maintained by local counsels on aging (G.L. c. 40, § 8);
- Unemployment insurance information (G.L. c. 151A, § 46);
- Student records (G.L. c. 71, §§ 34D & 34E);
- Records of hazardous waste facilities (G.L. c. 21C, § 12);
- Hospital records (G.L. c. 111, § 70); and
- Records of public assistance for the elderly (G.L. 19A, § 23).

Even where the records sought do not fall specifically into one of these exempted statutes, custodians should consider denying public records requests if the data and documentation requested regarding internal computer systems and information technology may lead to the disclosure of such sensitive materials.

December 4, 2021

MIIA Risk Management
Work Safe. Be Safe.