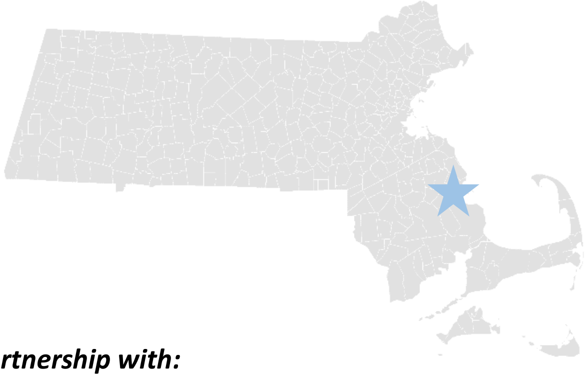
TOWN OF KINGSTON

CYBER SECURITY BEST PRACTICE | JULY 2017

EXECUTIVE SUMMARY

The Town of Kingston has adopted the Cyber Security best practice as part of a Community Compact agreement signed with the Baker-Polito Administration in January of 2016. Leveraging Community Compact funding, the Town retained the services of JDCSS, Inc. to assess their cyber security readiness via a comprehensive security assessment report. At the end of 2016, JDCSS, Inc. completed their work and delivered the report to Town leadership detailing their findings and recommendations.



In partnership with:

COMMUNITY PROFILE

The Town of Kingston is a coastal community in Southeastern Massachusetts. Prior to its incorporation in 1726, the Town was a part of the Plymouth colony, home of the Pilgrims' settlement. Today, Kingston is primarily a residential area with an active historical community. There are a small number of professional fishermen and cranberry growers still in business.

Population is 12,629 residents*
Annual Budget is $43.4M (FY 2017)
Median Household Income is $70,045*

**As of 2010 census*

Photo Credit: Flickr – Jennifer Macaulay at Rocky Nook Park in Kingston, Massachusetts

BACKGROUND

Many municipalities are attempting to modernize their technology environments to match the needs and expectations of their employees and constituents. Kingston is no different. The Town has experienced various technology challenges in the past, including a virus which impacted the Town twice, causing some files to be lost. While the Town tried to address gaps through part-time IT staff and consultants, with increasing technology demands and cyber security threats, they realized full-time IT support would be needed.

Marie Grossmann, Kingston's new IT Manager, has taken multiple steps to improve the Town's technology, including changes on the desktop, network, and server levels. Marie is also rolling out VoIP[1] and VPN[2] technologies across the Town. By leveraging a Community Compact grant for a security assessment report, Marie hopes to develop a plan to secure the Town's existing technology and ensure security of these new investments in technology moving forward.

PROJECT PROCESS

JDCSS, Inc. delivered a comprehensive cyber security report based on findings from the following activities:

- Interviews with key staff members in charge of policy, administration, day-to-day operations, system administration, network management, and facilities management.

- A visual walkthrough of the facilities with administrative and facilities personnel to assess physical security.

- A series of network scans to enumerate addressable devices and to assess each system's available network services (and an external scan conducted from the outside).

- Review of the configuration and security with IT personnel.

Although the Town has multiple departments and buildings, the focus of the assessment was the "Kingston Town House" which contains many Town departments including the Board of Selectmen, the Town Clerk, Town Finance, and the Town Administrator's office. As Marie expands the network, she plans on conducting further assessments to validate the improvements are aligned with security best practices.

[1] Voice Over Internet Protocol, the routing of voice calls over the Internet instead of standard copper telephone lines

[2] Virtual Private Network, which extends a private network across a public network, and enables users to send and receive data across shared or public networks

Photo Credit: Flickr – Chris Devers at Jones River in Kingston, Massachusetts

The report on the Kingston Town House is divided up into multiple sections, including:

Asset Identification	Threat Assessment	Laws, Regulations, and Policy
Personnel	Network Security	System Security
Application Security	Operational Security	Physical Security

The report contains detailed findings in each of the aforementioned areas and includes remediation recommendations. Certain high importance areas and remediation recommendations are included in a “Top Ten List” which highlights the most urgent issues discovered in the assessment. Marie is working to remediate the issues documented in the “Top Ten List” and in the other detailed sections of the assessment as well.

The report also includes several technology policies which have been rolled out in Kingston, governing things like wireless access by employees and guests, passwords, and VPN access. These policies (including the Password Protection Policy attached to this report as an appendix) are helpful as the technology environment becomes more advanced.

RECOMMENDATIONS & CONCLUSION

MassIT applauds Kingston’s proactive approach towards securing the Town’s growing technology environment. Marie’s work will be extremely important for the Town’s long-term information technology security. The report provided by JDCSS can help provide the foundation for future improvements which will benefit constituents and Town employees. MassIT recommends that Kingston continue to remediate the issues identified in the report, continue to make ongoing, strategic investments in technology and ensure that IT policies are added and/or updated as the technology landscape within the Town evolves.

Appendix A

Password Protection Policy

1. Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of the Town of Kingston's resources. All users, including contractors and vendors with access to Town of Kingston systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3. Scope

This policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Town of Kingston facility, has access to the Town of Kingston network, or stores any non-public Town of Kingston information.

4. Policy

4.1 Password Creation

4.1.1 All user-level and system-level passwords must conform to the Password Construction Guidelines.

4.1.2 Users must not use the same password for Town of Kingston accounts as for other non-Town of Kingston accounts (for example, personal ISP account, option trading account, benefits or bank accounts, and so on).

4.1.3 Where possible, users must not use the same password for various Town of Kingston access needs.

4.1.4 User accounts that have system-level privileges granted through group memberships or programs such as Munis must have passwords for those that are unique from the passwords of all other accounts held by that user to access system-level privileges.

4.1.5 Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to log in interactively. SNMP community strings must meet Password Construction Guidelines.

4.2 Password Change

4.2.1 All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis.

4.2.2 All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every six months. The recommended change interval is every four months.

4.2.3 Password cracking or guessing may be performed on a periodic or random basis by the IT team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

4.3 Password Protection

4.3.1 Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential Town of Kingston information. Kingston Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.

4.3.2 Passwords must not be inserted into email messages, Alliance cases, or other forms of electronic communication.

4.3.3 Passwords must not be revealed over the phone to anyone.

4.3.4 Do not reveal a password on questionnaires or security forms.

4.3.5 Do not hint at the format of a password (for example, "my family name").

4.3.6 Do not share Town of Kingston passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.

4.3.7 Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.

4.3.8 Do not use the "Remember Password" feature of applications (for example, web browsers).

4.3.9 Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

4.4 Application Development

Application developers must ensure that their programs contain the following security precautions.

4.4.1 Applications must support authentication of individual users, not groups.

4.4.2 Applications must not store passwords in clear text or in any easily reversible form.

4.4.3 Applications must not transmit passwords in clear text over the network.

4.4.4 Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

4.5 Use of Passwords and Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

5. Policy Compliance

5.1 Compliance Measurement

The IT team will verify compliance to this policy through various methods, including but not limited to periodic walk-throughs, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the IT team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies, and Processes

Policy Setting

- Enforce password history 6 passwords remembered
- Maximum password age 180 days
- Minimum password age 30 days
- Minimum password length 8 characters
- Password must meet complexity requirements Enabled
- Store passwords using reversible encryption Disabled

Password Complexity

Password complexity policies are designed to deter brute force attacks by increasing the number of possible passwords. When password complexity policy is enforced, new passwords must meet the following guidelines:

- The password does not contain the account name of the user.
- The password is at least eight characters long.
- The password contains characters from three of the following four categories:
    - Latin uppercase letters (A through Z)
    - Latin lowercase letters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphanumeric characters, such as exclamation point (!), dollar sign ($), number sign (#), or percent symbol (%).

Passwords can be up to 128 characters long. You should use passwords that are as long and complex as possible.