RESOLUTION 2019–135

RESOLUTION OF THE MAYOR AND BOROUGH COUNCIL OF THE BOROUGH OF MOUNT ARLINGTON, IN THE COUNTY MEMORIALIZING A TECHNOLOGY PRACTICE POLICY

WHEREAS, the Borough of Mount Arlington would like to memorialize the attached Technology Practice Policy adopted in accordance with Technology Proficiency Standards, as recommended by the New Jersey Municipal Excess Liability Joint Insurance Fund Cyber Risk Management Program.

NOW, THEREFORE, BE IT RESOLVED, by the Mayor and Borough Council of the Borough of Mount Arlington, County of Morris, State of New Jersey, that the above referenced Technology Practice Policy be memorialized.

I HEREBY CERTIFY this to be a true and correct Resolution of the Mayor and Borough Council of the Borough of Mount Arlington, and adopted on September 3, 2019.

L. Dwyer
Acting Borough Clerk

BOROUGH OF MOUNT ARLINGTON

TECHNOLOGY PRACTICE POLICY

Purpose: To establish as policy certain information technology practices. Further, compliance with various practices will enable the Borough of Mount Arlington to claim a reimbursement of a paid insurance deductible in the event the member files a claim against Borough of Mount Arlington's cyber insurance policy, administered through Morris County Municipal Joint Insurance Fund.

A. **Technical Operations**
   1. **System and data back-up practices:** Borough of Mount Arlington will implement backup practices that meet the following as a minimum standard, or will implement recommendations of a qualified information technology advisor who, after consideration of Borough of Mount Arlington's information technology needs, recommends an alternative, which shall be fully documented.
      a. Daily incremental backups or the use of standardized system images or virtualized desktops, with at least 14 days of versioning on off-network device for data files
      b. Weekly off-network full backups of all devices:
         i. Use of non-versioned, synchronized cloud=based drives are not acceptable as backup solutions. Cloud-based drives used for backup must have a minimum of 14 days of versioned files.
         ii. A full back up of non-networked/standalone desk and laptop computers must include all storage drives
         iii. All backups are spot-checked monthly
         iv. Consult with third party application providers to ensure their data files are part of a backup practice
   2. **Security and System patching:** all operating and application software shall be updated on a timely basis with latest versions as released, particularly as related to security updates. Outdated or non-supported operating systems and software shall not be used unless there is not practical alternative available, in which case, appropriate steps shall be taken to mitigate potential security threats. System administrators shall coordinate patching with applications maintained or managed by third parties to ensure upgrades will not disable their applications. When upgrades cannot be applied, appropriate action shall be taken to prevent the system or application from security exploitation.
   3. **Defensive Software** shall be installed and operative on all computing devices as follows:
      a. For all desktops and laptops devices: antivirus and an enabled firewall
      b. Mail Server: anti-spam and anti-virus filters
      c. For network servers that connect to the internet: an active firewall on all open ports, unused ports closed; and anti-virus, anti-malware software running
      d. All Microsoft Office applications are set to all downloaded files in "Protected Mode"

4. **Server Security:** al servers are protected from unauthorized access by means of a secured cage, locked cabinet (with sufficient airflow) or other physically secure means to ensure that only authorized users have access to it.
5. **Access privilege controls and policies** are in place and maintained to ensure that: 1) users with administrator rights are limited to those that need them; 2) that other users only have access to those services they need for day to day activities; 3) that access is removed when it is no longer needed or when an employee separates from service; and 4) access rights are periodically reviewed to ensure compliance. The Borough Administrator shall work with the Borough Technology Contractors to ensure that system access needed by new employees is provided on a timely basis, and that notice of termination of employees is provided and acted upon by the Borough Technology Professionals prior to notice provided to the employee.
6. **Security Incident Response:** Appropriately trained staff or contractors are available to support the Borough of Mount Arlington's technology and to timely respond to security incidents.

B. Employee-based Cyber Security Practices

1. All computer users shall receive annual training of at least one hour annually, in email and website malware identification, password construction, identifying security incidents and social engineering attacks.
2. Employees are required to use unique passwords or passphrases made up of at least 8 characters, changed periodically, but at least annually. Passwords/phrases shall be at least 8 alpha-numeric characters, with incidental upper- and lower-case letters and symbols.
3. Files that contain protected data shall be password protected or be encrypted when the files are stored or transferred to others, regardless of the storage medium or means of transfer. Examples of protected data includes social security numbers, birthdates, driver's license number, health insurance numbers, etc. Practices shall include ensuring that more than one employee is aware of the password or passphrase used to encrypt these files.

C. Technology Management Practices

1. Mayor and Council shall ensure that technology policy decisions (i.e. risk assessment, planning and budgeting) are made with input from staff or advisors that possess appropriate technological expertise. This can by any combination of officials, employees, contractors/consultants as they determine necessary.
2. Borough Administrator shall approve and implement a cybersecurity incident response plan to direct staff and guide IT management decision making when a cybersecurity incident takes place.