RESOLUTION G2018-90

RESOLUTION ADOPTING A DISASTER RECOVERY AND CYBER LIABILITY POLICY FOR SYMMES TOWNSHIP

WHEREAS, the State Auditor's Office has identified the need for Symmes Township to adopt a disaster recovery policy for the township so that documents and the contents of the township's server will be retained in case of an emergency or complete disaster;

WHEREAS, the Board discussed the need to adopt a policy in previous meetings after the audit was released in January of this year indicating the need to adopt one; and

WHEREAS, the Board of Trustees, Symmes Township. Hamilton County, Ohio, has reviewed the new Disaster Recovery Policy which includes how the documents and the contents of the township's server will be retained in case of an emergency or complete disaster; and

WHEREAS, the Township Administrator recommends the adoption of this new policy in order to ensure that the contents of the township's server will be retained in case of an emergency or complete disaster and to meet the requirements set by the State of Ohio.

NOW, THEREFORE, BE IT RESOLVED that the Board of Trustees of Symmes Township, Hamilton County, Ohio:

Section 1. The Symmes Township Disaster Recovery and Cyber Liability Policy attached hereto and incorporated herein as Exhibit "A," is hereby adopted as the Disaster Recovery Policy.

Section 2. The Disaster Recovery and Cyber Liability Policy shall replace and supersede any other formal or informal practice or procedure now in place with regard to back-ups of township documents.

Section 3. The Disaster Recovery and Cyber Liability Policy shall be reviewed as needed.

Section 4. Upon majority vote does hereby dispense with the requirement that this Resolution be read on two separate days and hereby authorizes the adoption of this Resolution upon its first reading.

Section 5. This Resolution shall take effect and be enforced from and after the earliest period allowed by law.

Section 6. Finds and determines that all formal actions of this Board concerning and relating to the passage of this resolution were taken in open meetings of this

Board, and that all deliberations of this Board and any of its committee that resulted in such formal actions were taken in meetings open to the public, incompliance with all legal requirements, including (without limitation) Ohio Revised Code §121.22, except as otherwise permitted thereby.

ADOPTED DECEMBER 4, 2018 – RESOLUTION G2018-90

Vote Record: Mr. Bryant ____ Mr. Beck____ Ms. Leis____

BOARD OF TOWNSHIP TRUSTEES:

_____
Kenneth N. Bryant, President

_____
Philip J. Beck, Vice-President

_____
Jodie L. Leis, Trustee

ATTEST:

_____
Carol A. Sims, Fiscal Officer

APPROVED AS TO FORM:

_____
Kevin McDonough, Law Director

SYMMES TOWNSHIP

DISASTER RECOVERY AND CYBER LIABILITY POLICY

Adopted – December 4, 2018

PURPOSE

The goal of this policy is to outline various measures that Symmes Township will take in order to mitigate any potential cyber threat, data breach or disaster. This policy will also outline internal procedures for data storage and user access.

INTERNET

Symmes Township employees will have access to the internet for general use during the daily operations. In order to protect employees and the Township's cyber infrastructure, the entire Township network shall be behind a firewall preventing unauthorized access from outside of the Township network. Firewall restrictions shall be configured on the most restrictive basis and then subsequently configured to allow necessary traffic to and from the outside network as requested, and approved.

EMAIL

Employee's will be provided with a Symmes Township Email address. In order to prevent issues with Email and to comply with Open Records and HIPPA laws, the following measures shall be in place:

1. All Township Email transmissions shall pass through a virus and spam filter.
2. All Email originating from Symmes Township shall be appended as such:
    a. Confidentiality Notice – the content of this communication, along with any attachments, is covered by federal and state law governing electronic communication and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of the information contained herein is strictly prohibited and punishable by law.

NETWORK SECURITY

In order to secure the Township's cyber network, the following measures are in place:

1. The Township network shall require users to maintain a password with a minimum complexity and to be updated every one hundred eighty (180) days. The end of this one hundred eighty (180) day period will result in a mandatory

password change for all Township network users. Individuals will not be able to access the Township network until their password is updated.

2. A network account lockout policy shall be implemented to affect any particular user account to lock, thus preventing access to the network for that account, after a sequence of three invalid password attempts. Only the IT Contractor may unlock the offending account after investigating the reason why the invalid password attempts were made.
3. File and server user access shall default to the most restrictive permission/rights. Appropriate file and/or server access permissions shall be granted (or denied) to all Township network users as necessary and approved by the IT Contractor and/or Township Administrator.

HARDWARE SECURITY

The Township maintains a robust network of computers, printers, servers, firewalls, filters, switches and other equipment. In order to secure these items, the following measures are in place:

1. All Township network servers, firewall, filters and switches shall be locked in a secure server room or closet, with limited access only to necessary personnel.
2. All other Township PC's, laptops, printers, etc. shall be inventoried and accounted for by location, serial number, and make/model.
3. All Township PC's will have basic user rights assigned. Local PC Administrator rights shall be given to a user for a particular PC on a per case basis upon approval.

DATA SECURITY

Governments collect and receive a large amount of data. Some of this data is public record and other pieces of date are considered private and not available to the general public. The above measures for network security are intended to protect this data. However, there is also a risk that this data may be deleted or lost. In order to protect this data from exposure and to ensure that data is not lost, the following measures are in place:

1. All Township data will be maintained on a disk storage array configured in RAID 5 hardware disk redundancy.
2. The disk storage array shall be secured in a locked, climate controlled, server room.
3. All Township data shall be backed up according to a rotating retention schedule as deemed appropriate by the IT Contractor and/or Township Administrator based on current available recovery space on existing infrastructure.
    a. In the interest of disaster recovery, the backup storage device shall be located in a separate building in a secured location.

b. Tests of the Township's backups shall be performed once per month to verify successful operation of the backup media and schedules.
c. A third backup of data shall be completed by virtual image of the server via the cloud.