TOWNSHIP OF BYRAM
RESOLUTION NO. 064 – 2020

RESOLUTION BY THE BYRAM TOWNSHIP MAYOR AND COUNCIL ADOPTING THE CRYPTOGRAPHIC CONTROLS POLICY AND THE MOBILE DEVICE POLICY

WHEREAS, Byram Township received a Statewide Insurance Fund Grant to enhance and sustain our cyber security posture as well as to ensure that our information system is secure and protected from cyber incidents; and

WHEREAS, in our Cyber Gap Assessment completed by PivotPoint Security, the lack of having a cryptographic controls policy and a mobile device policy were identified as high-risk priorities; and

WHEREAS, the Township has worked with its IT provider to develop these policies.

NOW, THEREFORE, BE IT RESOLVED, that the Mayor and Council of the Township of Byram hereby adopts the attached Cryptographic Controls Policy and the Mobile Device Policy; and

BE IT FURTHER RESOLVED by the Mayor and Council of the Township of Byram that these policies are incorporated, effective immediately, into the Byram Township Employee Handbook.

BYRAM TOWNSHIP COUNCIL

	Councilman Bonker	Councilwoman Franco	Councilman Gallagher	Councilman Roseff	Mayor Rubenstein
Motion			X		
2nd				X	
Yes	X	X	X	X	X
No					
Abstain					
Absent					

ATTEST: I certify that the foregoing resolution was adopted by the Byram Township Council at a meeting held on April 21, 2020.

Doris Flynn, RMC
Township Clerk

Cryptographic Controls Policy

Prepared for Byram Township and Police Department by navitend

1 CONTENTS

2 OVERVIEW

Cryptographic controls help to mitigate the risk of data being compromised. The underlying cryptographic technology covered by this policy is encryption.

3 PURPOSE

The purpose of this policy is to ensure that employees do not transmit sensitive information, personally identifiable information (PII), or protected health information (PHI) in an unencrypted fashion.

4 SCOPE

This policy applies to all employees of Byram Township and PD.

5 GLOSSARY OF TERMS

1. Encryption: a cryptographic method that converts an original message of regular text into encoded text. The text is encrypted by means of an algorithm (type of formula). If information is encrypted, there is a low probability that anyone other than the receiving party who has the key to the code or

access to another confidential process would be able to decrypt (translate) the text and convert it into plain, comprehensible text.

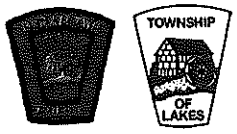
2. Mobile Device: Laptops, phones, tablets, smartwatches, thumb drives, and any other device that is mobile as its typical mode of operation.
3. Data transmission: Data transmission is the movement of data outside of the Byram network in any manner, including email and file-sharing websites.
4. Personally, Identifiable Information (PII): Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available - in any medium and from any source - that, when combined with other available information, could be used to identify an individual.
5. Protected Health Information (PHI): health information that is individually identifiable (see definition of Personally Identifiable Information above).

6 POLICIES

1. Sensitive information, Personally Identifiable Information, and Protected Health Information shall not be transmitted in an unencrypted manner.
   1.1. To encrypt an email sent outside of the Byram organization, make sure the word "encrypt" appears in the subject-line of the email.
   1.2. Emails sent within the Byram organization are encrypted automatically.
   1.3. Certain emails will be automatically encrypted if they contain certain sensitive types of information.
2. Information transmitted into and out of the Office 365 system through the web browser is automatically encrypted using https technology.
3. The following types of devices shall be encrypted using full-disk encryption technology:
   3.1. Township-issued laptops
4. No Township files should be stored on non-Township-issued devices.

7 CONTROLS

1. Cloud-based encryption management software shall verify full-disk encryption is in-use on Township-issued laptops



8 ENFORCEMENT

This policy shall be enforced by Township management. Violation of this policy may result in disciplinary action, up to and including termination.

9 DOCUMENT HISTORY

Version	Date	Summary
1.0	04/14/2020	Initial Version of Policy

Mobile Device Policy

Prepared for Byram Township and Police Department by navitend

1 CONTENTS

2 OVERVIEW

Mobile Devices carry with them an inherent security risk to Byram Township & PD. There are several steps that can be taken to mitigate that risk.

3 Purpose

The purpose of this policy is to secure the use of mobile devices in-use at Byram.

4 SCOPE

This policy applies to all employees of Byram that use an issued mobile device.

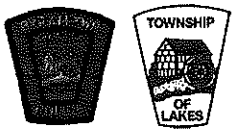
5 GLOSSARY OF TERMS

- Mobile Device: Laptops, phones, tablets, smartwatches, and any other device that is typically mobile.
- Byram Twp. Data: Includes, but it not limited to, the following items:
  - Network
  - Shared drives

- Applications
- Email
- WiFi network
- Printers
- Any other information technology item belonging to Byram

6 POLICIES

1. Software requirements
   1.1. All Township-issued laptops must have the management and protection tools provided by the Township's IT-vendor.
      1.1.1. The required software is the Remote Monitoring & Management (RMM) agent, Sophos Central Encryption agent, and the Sophos Intercept X Advanced endpoint protection agent.
   1.2. The operating system of the mobile devices shall not be tampered with or altered in any way, including "rooting" the device or changing the underlying firmware/software.
   1.3. Software may not be installed on the mobile device without authorization from the Township.
   1.4. If any Office 365 software is accessed from the device, it shall use the Byram user's E3 licensing.
2. Data Storage
   2.1. Users shall not store company data, other than email data, locally on their non-Township-issued devices.
3. Data Backup
   3.1. User of mobile device is responsible to ensure that important data is appropriately backed up.
4. Encryption
   4.1. All Township-issued laptops shall be encrypted using full-disk encryption.
   4.2. For iOS and Android devices, any default built-in full-disk encryption technology shall be used and not disabled.
   4.3. For Windows devices, built-in Bitlocker full-disk encryption technology shall be used via Sophos Central Encryption agent.
5. Password protection
   5.1. All mobile devices shall be password protected.
   5.2. For iOS and Android devices, a 4-digit PIN password is the minimum acceptable password.
   5.3. For Windows devices, a strong, unique, and complex password is required.
6. WiFi Usage
   6.1. Secure WiFi networks are preferred over insecure.
   6.2. Township employees shall not use public unsecured WiFi networks to access company files.
7. Physical security
   7.1. Devices shall always be physically secured when not attended.
   7.2. If a device is lost or stolen the employee shall immediately notify the Township so that appropriate action can be taken.
   7.3. Unauthorized access to mobile devices shall be reported to the Township immediately.



7 CONTROLS

1. The Township may conduct random spot-checks for compliance on Township-issued mobile devices.
2. Township will educate employees on Mobile Device Policy and employees are responsible for compliance on all mobile devices they use to conduct Township business.
3. Encryption
   3.1. For Township-issued laptops, Sophos Central Encryption shall be used to enforce and manage full-disk encryption.
4. Password protection
   4.1. For Township-issued laptops, password complexity shall be enforced using Group Policy Objects on the Domain Controller server.

8 ENFORCEMENT

This policy shall be enforced by Township management. Violation of this policy may result in disciplinary action, up to and including termination.

9 DOCUMENT HISTORY

Version	Date	Summary
1.0	04/14/2020	Initial Version of Policy