MOPAC | MAYOR OF LONDON
OFFICE FOR POLICING AND CRIME

Digital Security Policy

Introduction

1. This document sets out the digital security settings MOPAC has in place to protect its IT equipment and the information stored on them.

Email encryption

2. The Greater London Authority (GLA) have implemented an email encryption solution called Forcepoint which means that all of MOPAC's outgoing emails are now encrypted to the government recommended standard of TLS 1.2*.

3. This is also the standard used for email communications between the MPS and MOPAC.

4. If the recipient uses commercial email applications such as Microsoft like MOPAC does, emails will be encrypted to this standard. However if they use lesser known shareware/freeware mail applications and it is detected that it doesn't support TLS 1.2, the outgoing email will not be encrypted.

*Transport Layer Security (TLS) Protocol. This protocol is an industry standard designed to protect the privacy of information communicated over the Internet. TLS assumes that a connection-oriented transport, typically TCP, is in use.

Device encryption

5. All of MOPAC's laptops and Surface Pros are encrypted to 256-bit AES encryption. The main purpose is to encrypt the hard disk to protect the data from unauthorised access such as when a device is stolen.

6. When outside the building, there is an increased risk of theft or loss and for anyone who has possession of the device, unless they know the password to login in, they will not be able to get access to the drive. Even if the drive is taken out of the device, if the drive is encrypted (BitLocker installed and enabled), the data will be protected.

7. To add further protection, there are also the changes to password length and format (see below), and the introduction of Multi-Factor Authentication (MFA) for accessing Office 365 on the Cloud.

Anti-virus

8. As part of the work in ensuring that the GLA is protected from malicious cyber-attacks the Technology Group (TG) have installed an anti-virus system called CrowdStrike to protect our Surface Pros and laptops.

9. However, if you have a GLA laptop at home that only connects remotely to the GLA network via Citrix you may need to bring it in. TG will provide more guidance on this shortly.

Mobility Management Tool

10. MOPAC utilises Microsoft Intune to manage out corporate mobile phone devices to access corporate information such as emails and documents.

11. MOPAC iPhone devices are set up with strong security settings within Intune which incorporates conditional access and MFA as well as restrictions such as blocking airdrop, pairing with Apple watch, multiplayer gaming, movies, and transferring of corporate contents to unmanaged apps, as well as the following:

    - Password: 6 numeric digits
    - Wipe device after 10 failed sign-in
    - Notification while device is locked: yes
    - App store: yes
    - Siri: yes
    - Delete apps: yes

Password policy

12. The GLA sets the password policy for MOPAC and they have a minimum 12 characters and is not required to be changed in the future. The reasoning behind this is that regularly changing passwords result in an increased risk of individuals writing down their passwords, resulting in a less secure approach.

13. The format of the passwords is that they need to include characters from three of the following groups:

    - Uppercase alphabet characters (A-Z)
    - Lowercase alphabet characters (a-z),
    - Arabic numerals (0-9)
    - Nonalphanumeric characters (for example, !$#,%).

14. All staff are advised to adhere to the following guidelines with regards to password:

    - Choose a memorable password that is long but is easy to remember, this can be a phrase or combination of three random works. Further tips and advice are available here: https://www.getsafeonline.org/protecting-yourself/passwords/

- Ensure your MOPAC password is unique and not used for any other purpose e.g. personal email accounts.
- Passwords should not be written down in a way that could be read by anybody else and become compromised.
- Do not share or reveal your password to others. Very rarely, the TG Service Desk may need the passcode to a user's phone or network password to resolve an issue on your behalf. Where this is the case, make sure you have verified that you are really talking to a Service Desk Officer and, once they have completed their work, change your password or any other access codes.
- Take extra care when entering your password to ensure the system/website is legitimate and not a 'phishing attach'. Office 365 logins will always be to the domain https://login.microsoftonline.com/. Further guidance is available here on the GLA intranet: http://intranet.london.gov.uk/node/14247
- If you have any concerns or doubt that your password may have been compromised please change it as soon as possible and notify the TG Service Desk.

Remote access

15. MOPAC uses Microsoft's MFA to access with staff corporate iPhones used for receiving authentication requests via the Authenticator application which allows staff to accept the login request without having to type in any numbers.

Version	Date	Author	Description of change
0.1		[redacted]	First Draft
0.2	27/02/2020	James Bottomley	Additional detail on version control. Review of dates for retention and disposal.