Board Paper (23) 07

Meeting: Legal Services Board

Date: 24 Jan 2023

Item: Paper (23) 07

Title: Cyber security – personal devices

Author(s): **Donella Williams, Stuart Hamill**

Status: Official

Introduction: Purpose of the paper/ Issue

1. To inform Board members of the changes to the LSB's Information Technology (IT) policy, so that it meets recognised standards on cyber security. This will mean material changes for personal device usage which will mainly impact Non Executive Directors and Consumer Panel members accessing LSB systems. This is being implemented to minimise cyber risk to the LSB's data and to ensure we are compliant with the additional requirements of the Cyber Essentials Plus (CE+) certification.

Background

2. To obtain the cyber security certifications, the LSB are preparing for a cyber security audit by an independent auditor. There are 2 steps: Cyber Essentials (CE) and Cyber Essentials Plus (CE+)). The purpose of the audit is to gain certification that states the organisation has mitigations in place to protect itself from cyber threats. The plan is to complete CE by mid February and CE+ by mid March in time for year end.

3. To prepare for the audit, we undertook a cyber remediation project with our IT provider Rock and have reviewed and made updates to our IT security policy and the ways executive colleagues and non-executive directors access LSB systems.

4. Rock have made key changes to our security (outlined in Annex A) which includes enabling multi factor authentication (MFA) and updating the requirements for personal devices that are used to access LSB data via apps such as Microsoft Outlook and Microsoft Teams to improve our IT security and to be able to successfully pass the cyber security audit.

Discussion

Key changes

Mobile device management and personal device usage

5. LSB obtained the CE+ certification for the first time in 2021. However the CE+ specification has now been expanded for personal devices, as they have been reviewed as a key security risk to organisational data. The new requirement means that all mobile personal devices that access LSB data (laptops, tablets, mobile phones) are required to have Mobile Device Management (MDM) installed. MDM is critical as it allows individuals to use their own devices while covering any potential cyber and data security gaps.

6. MDM is a process of managing mobile devices, in terms of usage and security. MDM is managed by Rock via software called Intune. Rock creates and configures security policies through Intune which pushes those policies on to the mobile devices, causing security measures to be managed by Rock ensuring the personal device is protected. It also remotely secures mobile devices if they are lost or stolen. Rock will not be able to access any personal data on any device that has MDM installed.

7. Rock have implemented the following security policies that are required to have MDM installed and to allow users to access their LSB accounts on the personal device:

    a) Passcode enforcement (with minimum 6 characters)

    b) Passcode needs to be changed after 1 year

    c) Alerts and restrictions for devices trying to bypass restrictions with jailbreaking (installing software other than what the manufacturer has made available for that device)

    d) Latest version of OS that is compatible with that device

8. Once the MDM app is installed, Rock will have a list of all devices that access the LSB IT system, including essential information such as the device name, model, serial number, IMEI and OS version.

9. From 1st February all individuals who use their personal devices to access LSB data will be required to install the MDM app (Intune Company Portal). This app requires all users have the latest version of the operating system that is compatible with the device installed, as this has the highest security measures and protects your device and any LSB data from potential security threats. If the device is lost or stolen then data can also be wiped remotely by Rock.

10. The Company Portal app can only be linked to one organisation per device (due to conflicting security policies). Therefore, if the app is already installed

on the device as it is required by another organisation, we can provide a suitable LSB device to enable secure access to the LSB account.

11. In the event a personal device is lost or stolen, this will need to be immediately reported to the Head, Finance & IT or Corporate Projects Manager who will notify Rock as they are able to support with the protection of your LSB account and therefore LSB systems.

Multi-factor Authentication (MFA)

12. We have now enabled MFA, which is an authentication method where users are granted access to a system after presenting two factors to access the system (e.g, password and code sent to a registered phone number). This provides extra security in a potential instance where passwords are compromised.

13. When logging in you may occasionally be required to provide both your username and password as well as a code which will either be sent to the phone number linked to your account or a code that is provided via the Microsoft authenticator app (iOS/android).

IT policy updates

14. We have updated the personal device use section in our IT policy and now request that all who access accounts on our systems via personal devices must:

a) Have their devices protected by a password/pin:

- minimum six characters for mobile phones
- minimum eight characters for devices with a keyboard (desktop/laptop)

b) Any applications installed must be kept up to date. All updates should be applied within 14 days

c) Have an up-to-date antivirus software or app installed

d) The device must run a current version of its operating system and must also have a latest/current security update installed. A current version is defined to be one for which security updates continue to be produced and made available to the device (Windows 10/11, iOS or Android).

e) The device must be configured to “autolock” after a period of inactivity (no more than 15 minutes).

f) Software firewalls must not be disabled, or updates postponed. Devices capable of employing a software firewall will typically have this enabled by default and set to automatically update.

15. In addition to the minimum requirements above, the following recommendations will help further reduce risk:

a) Consider configuring the device to “auto-wipe” to protect against brute force password attacks where available.

b) Consider implementing remote lock/erase/locate features where available.

c) Do not undermine the security of the device (for example by “jail breaking” or “rooting” a smartphone)

d) Minimise the amount of restricted data stored on the device and do not store any data classified as confidential or above.

e) Be mindful of the risks of using open (unsecured) wireless networks. Consider configuring your device not to connect automatically to unknown networks.

f) If a personally owned device needs to be repaired, ensure that the company you use is subject to a contractual agreement which guarantees the secure handling of any data stored on the device.

g) If no longer required devices must be disposed of securely, removing any LSB data before disposal (see Annex X) for more details).

h) Do not leave mobile devices unattended where there is a significant risk of theft.

i) Be aware of your surroundings and protect yourself against “shoulder surfing”.

Next steps

Cyber Essentials assessment – w/c 6th February

Cyber Essentials Plus audit – w/c 20th February

Cyber Essentials Plus certification – March 2022

Annexes

Annex A – Cyber remediation project tasks
Annex B – How to perform master factor reset on devices

Freedom of Information Act 2000 (FoI)		
Para ref	**FoI exemption and summary**	**Expires**
None	None	None