Mobile Device Security Policy

(With Mobile Device Management)

Criminal Justice Secure eMail Service (CJSM)

This document provides an overview of how to configure mobile devices using Mobile Device Management (MDM) to securely access information transmitted through CJSM. It covers platform specific guidance for the current version of Android and all versions back to Android 4.3 or later, iOS (Apple devices – iOS 7 or later) and Windows 8.1 or later devices.

This document provides the mobile device policy for all CJSM users, enabling the implementation of best practice security settings for the device using MDM, and will enable demonstration of compliance to the Terms and Conditions for connecting to the Criminal Justice Secure eMail Service (CJSM).

All organisations including users can choose to use Mobile Devices, but they own the risk for the data they transmit, and should manage this risk in line with their own organisation's security policies.

All organisations including sole practitioners with staff, and single users who wish to use mobile devices to access CJSM must read and acknowledge their understanding and agreement to the following:

1. All organisations should ensure that all CJSM connections are routed over a secure enterprise VPN to provide protection of the traffic as it transits the connection.

2. All mobile devices MUST be password protected. All organisations SHOULD ensure that Users use a strong (minimum) 9 character password made up of alphanumeric characters i.e. passwords must be a mix of upper and lower case alphabetic characters plus numeric and/or special characters. This must be changed at least every 90 days.

3. All organisations MUST ensure that full encryption is enabled on all mobile devices prior to being provisioned to users for connecting to the CJSM environment.

4. All organisations MUST ensure that the mobile device (For Android and Apple iOS) is configured to disable installation of third-party Apps. For Windows, all organisations should provide procedural controls (including AUP and SyOPs) which should be given to all users with clear instructions not to install applications that are not approved for legitimate business use.

5. All organisations MUST configure their mobile devices to implement the ‘auto lock’ screen feature to ensure that the mobile device implements a screen saver after it is left idle for some time. This should be set to a maximum of five minutes.

6. All organisations MUST ensure that users setup the Auto Erase data feature on their Mobile devices to help to protect their data if the phone is lost. The ‘Auto erase’ feature ensures that after a preset number of incorrect password attempts, the feature will erase the data on the mobile device and ensure that no one can read or access it. Users should set the number of passcode attempts to 10.

7. All organisations MUST ensure that secure configuration is used to lock down permissions given to Apps to shared storage areas to provide protection to data stored on the devices. Application whitelisting should be used to limit access rights for Apps on the Mobile device.

8. All organisations SHOULD ensure that the USB interface is disabled as an interface used for transfer of files and installation of Apps, and should only be used for charging the Mobile Device.

9. All organisations MUST ensure that they employ best practice anti-virus solutions within their MDM implementation to protect the mobile devices from malware attacks

10. All organisations MUST configure the devices to only use email accounts provisioned via MDM to access CJSM environment.

11. All organisations MUST provide the users with procedural controls (e.g. Acceptable Use policy (AUP)) to inform the user that Bluetooth should not enabled on their mobile devices, and users MUST not connect to untrusted WiFi connections (e.g. Starbucks, Airport WiFi).

12. All organisations MUST ensure that all software and security updates are applied to the MDM managed mobile devices as soon as they become available. All mobile devices should be updated with the most up-to-date version of the Operating System available.

13. All organisations MUST ensure that they enable the security features on the device which provides the ability to remotely lock, wipe and locate the mobile device – Android (‘Find My Mobile’), Windows 8 (‘Find My Phone’) and iPhone (‘Find My iPhone’). The MDM solution should be configured with the ability to remotely wipe the device if lost or stolen.

14. All organisations MUST ensure that they disable the ‘Auto Backup’ feature on their device, and this should be set up to a local backup feature that prevents the upload of personal and sensitive information to a service provider’s cloud storage area. Where possible, MDM Solutions should be used to disable the ‘Auto Backup’ feature including location services to

prevent the use of application tracking services by individual applications to release sensitive device information.

15. All organisations MUST implement MDM solutions that enable the detection of modification of configuration settings on the Mobile Devices. This should include the ability to lock down the device and prevent further use of the mobile phone in accessing the CJSM environment.

16. All organisations MUST provide the users with procedural controls (e.g. Security Operating Procedures (SyOPs)) to inform the user that mobile devices used to access CJSM MUST not be altered or adapted in any way (e.g. modifications to the base Operating System). If a user suspects that their device has been altered or adapted, the device must not be used to access CJSM, and the user MUST report this breach immediately to the Organisation who will notify the CJSM helpdesk.

17. All organisations MUST ensure that mail settings used to connect to CJSM are configured to support SSL or TLS encryption to provide protection of email messages to/from the CJSM mail services

18. I note that the MOJ reserves the right to audit my access to CJSM and my compliance with this policy and I confirm that I will cooperate with the auditors and audit process. I also note that the MOJ will provide at least 4 weeks' notice of any such audit (where appropriate). Furthermore, I understand that the Service may be subject to monitoring and action taken if any suspected unauthorised misuse is identified.

19. I understand that the MoJ reserves the right to terminate my connection to CJSM in the event that the above mentioned audit activity reveals significant shortfalls in good security practice (as specified within this document). Similarly, I understand that if the output of the audit activity points to remedial activity being required and I do not demonstrate progress in line with MoJ requirements, my connection with CJSM may be terminated.

Declaration:

As the local user representative/user I am fully aware of my responsibilities in relation to the use of the Service and the terms as set out in this Mobile security policy.

Name (please print)   Signature   Date   Position

(Organisation name) ______________________________

Please return the organisation version of this document to:
The CJSM Administrators, Egress Software Technologies Ltd, Unit 16 Quadrant Business Centre,
135 Salusbury Road, London, NW6 6RJ
Telephone via the CJSM Helpdesk 0870 010 8535/ 020 7604 5598
User signed copies of this document should be retained by the organisation and be available on request to the Ministry of Justice or their appointed representatives.