Mobile Device Security Policy

(Without Mobile Device Management)

Criminal Justice Secure eMail Service (CJSM)

This document provides an overview of how to configure mobile devices securely to 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, 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 mobile devices MUST be password protected. Users SHOULD 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. Windows Mobile users SHOULD configure their devices to have numerical passwords up to a minimum of 7 digits.

2. All mobile devices MUST 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.

3. All users MUST 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. This is applicable to Apple iPhone users only.

4. All users MUST ensure that full encryption is enabled on mobile devices which will be used to access CJSM. Users should follow setup

instructions for their mobile device on how to setup full encryption. This is applicable to Android users only

5. Users who want to use a mail app functionality to access CJSM mail on their mobile devices MUST ONLY use the built-in 'Mail' app available on the Mobile device.

6. All users MUST ensure that they do not install applications where there is no legitimate business need or run any applications from untrusted sources. For Android devices ONLY, users MUST ensure that they disable the security setting 'Untrusted Sources' to prevent the installation of apps from untrusted sources.

7. All users SHOULD employ best practice anti-virus solutions offered by the App store in protecting their mobile devices from malware attacks.

8. All users SHOULD ensure that Bluetooth is not enabled on their mobile devices, and users MUST not connect to untrusted WiFi connections (e.g. Starbucks, Airport WiFi).

9. Users MUST ensure that all software and security updates are applied to their 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.

10. Users MUST enable the security features on the device which provides the ability to remotely lock, wipe and locate their mobile devices – Android ('Find My Mobile'), Windows 8 ('Find My Phone') and iPhone ('Find My iPhone').

11. All users 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.

12. All 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 CJSM helpdesk.

13. All users SHOULD ensure that external memory devices (e.g. SD cards) are not used with devices used to access CJSM.

14. All users 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. Users should follow guidance in the Mobile device configuration/administration guide to implement this feature.

15. 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.
16. 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.