Creating a safer
Cambridgeshire

To: Business Coordination Board

From: Chief Constable

Date: 14 March 2017

Information Assurance

1. Purpose

1.1 The purpose of this paper is to update the Business Coordination Board ("the Board") and provide assurance on compliance with regards to Cambridgeshire Constabulary's policies and procedures relating to Information Assurance, including protecting information and managing risks related to the use, processing, storage, and transmission of information (digital and physical) or data and the systems and processes used for those purposes.

2. Recommendation

2.1 The Board is recommended to note the contents of this report.

3. Background

3.1 This paper provides an overview of the Information Commissioner's guiding principles with regard to information security and the governance arrangements. It also includes policies, procedures, and measures that the Constabulary has in place to manage information (digital and physical) and how this information is protected.

4. Current Status

4.1 Legislative Requirements

The following standards and legislation have been considered and applied to support compliance with the 7th Principle of the Data Protection Act 1998, and Code of Connection requirements:

- ISO 27000 series of standards
- NIST standards
- CESG architectural patterns

- CESG Cloud Security Principles
- CESG End User Device Guidance.

Relevant legislation has been considered in the security design (Data Protection Act 1998, Freedom of Information Act 2000, Regulation of Investigatory Powers Act 2000, Police and Criminal Evidence Act 1988, Protection of Freedoms Act 2012).

4.2 Relevant Policy

The relevant policies and procedures in place are shown in the table below.

College of Policing Authorised Professional Practice: • Management of Police Information (MOPI) • Sharing Police Information • Data Protection • Information Assurance	• BCH Information Management Strategy • BCH Information Management Policy • BCH Information Charter • BCH Privacy Impact Assessment Policy
HMG Security Policy Framework	BCH Authorised Use of Classified Information Procedure
BCH Information Assurance Policy	BCH Acceptable Encryption Policy
BCH Risk Appetite Statement	BCH Information Security Incident Response and Reporting Procedure
BCH Asset Classification and Handling Procedure	BCH Physical Security Policy including "Clear desk" procedure
BCH Secure Asset Sanitisation and Disposal Policy	BCH Removable Media Policy
BCH Cryptographic Policy	ICT Change Control Policy
ICT Patch Management Policy	BCH Professional Standards Policy
Specific system and device security operating procedures (SyOps)	BCH Business Continuity Policy

4.3 Security Controls (Digital and Physical)

The ISO 27000 series of standards, NIST standards, CESG architectural patterns, CESG Cloud Security Principles, and CESG End User Device Guidance have been considered and applied where appropriate. When compliance is not achievable or not appropriate, any associated risk is managed by the Senior Information Risk Owner. Controls, i.e., safeguards and countermeasures, have been applied in the following areas:

- Governance and information risk management: reporting mechanisms; policies; security operating procedures.
- Personnel security: vetting; training, education, and awareness; transaction monitoring; disciplinary procedures.
- Physical security: premises are assessed to government standards (HMG Security Policy Framework).
- Network security: boundary controls; configuration management; patch management; end point security; access control; malware protection; wireless network security; network monitoring; logical segregation of business domains (GSC); PKI management; compliance checking (annual IT Health Check and t-Scheme audit).
- Crypto security (audited audited by CESG).
- Secure acquisition and provisioning of technology assets.
- Removable media: central issue and tracking, with encryption the default unless there is an operational exception.
- Secure sanitisation/disposal of assets (digital and physical) to HMG IA Standard 5.
- Security Incident Management managed by BCH Information Management Department, with incidents escalated on the basis of risk to the Senior Information Risk Owner.
- Business continuity and disaster recovery plans are in place and subject to testing.

Evidence of compliance with the stated security controls is annually assessed by the Cabinet Office and Home Office through applications to connect to the Public Sector Network (PSN) and national police information systems.

4.4 Training, Education and Awareness

NCALT computer-based training packages are available to all .pnn domain users. The, topics personnel are encouraged to undertake are Data Protection, Management of Police Information and Information Assurance.

Policies are available to all personnel via the intranet.

BCH are deploying a tool (Metacompliance) to enable security messaging and user security policy acceptance.

4.5 Governance

The Director of Information is the Senior Information Risk Owner, reporting to the Chief Constable. The Director of Information's responsibilities include:

- Chairing the Information Management Board (IMB) and Information Assurance Board.
- Management of the Information Risk Register, including direction for risk mitigation activity or endorsement of risk acceptance as appropriate.
- Contribution to national police information assurance policy and endorsement of local information assurance policy.
- Executive lead of the Information Management Department (IMD).

Senior business leads are defined as Information Asset Owners, reporting to the Senior Information Risk Owner on matters relating to information risk.

The Information Security Officer reports to the Senior Information Risk Owner on matters relating to information risk.

5. Recommendation

5.1 The Board is recommended to note the contents of this report.

BIBLIOGRAPHY

Contact Officer	Ian Bell, Director of Information