

Report of the Chief Constable to the Chair and Members of the Audit Committee 16th December 2016

Executive Officer: Mr Iain Spittal, Chief Constable

Status: For Decision

Information Security Update

1. Purpose

- 1.1 The purpose of this report is to provide the Audit Committee with continued assurances that Cleveland Police has implemented the necessary technical, physical, personnel and procedural security controls to protect its information and satisfy national Information Assurance (IA) requirements that are pertinent to the government and policing. A high-level summary of information assurance activities that were performed in 2016 is detailed below.

2. Recommendations

- 2.1 It is recommended that Members note the content of the report and take assurance that the appropriate information security controls are in place.

3. Information Assurance Governance

- 3.1 Mandatory and specialist IA roles: Senior Information Risk Owner (SIRO), Information Asset Owners (IAO's), Information Security Manager, Data Protection Manager; have been appointed in accordance with the requirements of the Cabinet Office Security Policy Framework. In addition, the Office of the Police and Crime Commissioner has appointed an Information Asset Owner to provide the governance for PCC related data that is housed on the Force network.
- 3.2 Staff in mandatory and specialist IA roles have been trained and are aware of their security responsibilities.
- 3.3 Staff who routinely handle personal and/or sensitive personal data as defined by the Data Protection Act (1998) have completed a computer-based training package, which was a mandatory requirement for the introduction of the Government Security Classification Scheme.
- 3.4 An Information Security Board has been established and is chaired by the SIRO. Terms of Reference have been agreed and members have been appointed. The

Information Security Board meets on a quarterly basis and meeting records are maintained.

- 3.5 Information Assurance has been developed to the point that it is now a standing agenda item on board meetings.
- 3.6 The SIRO meets with the Information Security Manager on a fortnightly basis and provides timely guidance of IA activities/issues as they present themselves
- 3.7 An Incident Management framework has been implemented by the Information Security Manager with oversight from the SIRO, and IA related risks are recorded on the Strategic Risk Register. All security related incidents and weaknesses are notified, assessed, managed and recorded in accordance with ISO27002 Information Security Management System. Data Protection breaches involving the loss, theft and/or unauthorised disclosure of personal data are investigated by the Data Protection Manager and an impact assessment is conducted against the Information Commissioners Office referral criteria.

4. Compliance

- 4.1 The Force is registered with the Information Commissioners Office and ensures compliance with the Data Protection Act (1998) through the duties and responsibilities of the Data Protection Manager.
- 4.2 Approval has been granted by the Government Digital Service (GDS) for the Force to connect to the Public Services Network following the presentation of a satisfactory IA compliance submission.
- 4.3 Approval has been granted by the National Policing Information Risk Management Team (NPIRMT) for the Force to connect to the Public Services Network for Policing (PSNP) following the presentation of a satisfactory IA compliance submission.
- 4.4 A National Policing Community of Trust Connection Approval Certificate has been issued for the ongoing connectivity to the wider police services.
- 4.5 The Force has been awarded the Cyber Essentials Certification, which has demonstrated that it has a good level of technical, physical, personnel and procedural security control measures to reduce the likelihood of a cyber related attack on the network from the internet.
- 4.6 An annual IT Security Health Check was conducted by an external penetration testing company. Identified vulnerabilities were added to a Remediation Action Plan and mitigation work is ongoing. There are no significant vulnerabilities remaining from this work and the SIRO has been fully engaged with this work from an information risk management perspective.

5. Implications

5.1 Finance

There are no financial implications arising from the content of this report.

5.2 Diversity and Equal Opportunities

There are no diversity or equal opportunity implications arising from the content of this report.

5.3 Human Rights Act

There are no Human Rights Act implications arising from the content of this report

5.4 Sustainability

There are no sustainability implications arising from this report.

5.5 Risk

There are no risk implications arising from the content of this report.

Iain Spittal
Chief Constable