

Item 6

**Report to the Chair and Members of the Audit Committee**

**14th November 2019**

**Executive Officer: Mr Steven Graham, Assistant Chief Constable**

**Presenting: Dr Phil Brooke, Information Security Manager**

**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 government and policing. A high-level summary of information assurance activities that were performed in 2019 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 The force continues with a governance framework including specialist IA roles: Senior Information Risk Owner (SIRO), Information Asset Owners (IAO’s), Information Security Manager (ISM), and Data Protection Manager. The allocation of Information Asset Owners has been updated and remains important to future assurance work. A new member of staff was appointed to the role of GDPR Auditor and Deputy Information Security Officer allowing for proactive reviews of information workflows and to provide more resilience in the information security area.

3.2 The baseline training for all officers and staff currently comprises three e-learning packages. These are “Managing Information” (operation and non-operational), “Protecting information level 1” and “Government security classification”.

3.3 The ISM continued ISO27001 training and passed a Lead Auditor course which has proved valuable. The new GDPR Auditor has received specialist training in particular computer systems (CAID and PND) and is due for additional training.   
  
  
All IAOs are still expected to complete the “Protecting Information” level 2 course and are encouraged to consider the level 3 course.

3.4 An Information Security Board continues to meet. Particular issues include

i. the need to maintain a high level of patching across the full range of information assets;   
ii. improving the physical security of the sites, particular in respect of intruders into car parks and CSH; and   
iii. the need for better IT support for an information security management system, so we can improve our capability to carry information security governance activities.

3.5 After a number of role changes within the wider Force, the Information Asset Owners meetings have been restarted. IAOs are further supported by the GDPR Auditor.

3.6 The SIRO is currently ACC Steve Graham after a period of change. The head of DSE, Cristiana Emsley, is the Deputy SIRO. Five strategic risks were identified before the previous report and remain

i. loss/disclosure of paper documents;

ii. inappropriate disclosure electronically (e.g., email, social media);

iii. availability of critical computer systems;

iv. loss/disclosure of removable media; and

v. physical security of sites.

3.7 Security incidents continue to be recorded, assessed and reviewed by the ISM. Whether personal information is involved, the DPM makes an assessment in relation to notifying the Information Commissioner’s Office. Critical incidents are handled by “gold” groups.

3.8 The Information Security Policy was rewritten to make it more broadly applicable and easier to comprehend, along with new security operating procedures due to the agile/mobile working project.

**4. Compliance**

4.1 The Force is registered with the Information Commissioner’s Office and ensures compliance with GDPR and the Data Protection Act (2018) through the duties and responsibilities of the Data Protection Manager.

4.2 An annual IT Security Health Check (ITSHC) was conducted by an external penetration testing company in June 2019. The results were generally positive, although as expected some issues require remediation. Issues graded as “serious” and “high” have been fixed with few exceptions. ICT has been asked to provide a plan for the completion of the necessary remediation work, including all “medium” and “low” issues.

4.3 Preparation of the Force’s annual applications to the Government Digital Service (GDS) to continue to connect to the Public Services Network, and to the National Police Information Risk Management Team for our connection to   
  
the Public Service Network for Policing (PSNP) and Airwave will commence in November with an expectation of submitting the reports in December.

**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 new risk implications arising from the content of this report.

Phil Brooke

Information Security Manager

25 October 2019