Report to the Chair and Members of the Audit Committee
16th December 2021

Executive Officer: **Helen McMillan, Deputy Chief Constable**
Presenting: **Susan Haider, Head of Information Management and Data Protection Officer**

Status: For Information

Information Management 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. This report will also provide assurances around compliance with data protection legislation and areas of risk. A high-level summary of information assurance activities that were performed in 2021 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 (IAOs), Information Security Manager (ISM), Records Manager and Data Protection Officer (DPO is also the Head of the Information Management Unit).

The SIRO is currently DCC Helen McMillan. The strategic risks 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.

3.2 The GDPR Auditor and Deputy ISO continues to review existing and new workflows across the organisation, providing additional detailed information in relation to information risks.

3.3 An IT Security Officer (ITSO) has been recruited during this reporting period. The ITSO is working closely with ICT and other teams in relation to projects such as the printer uplift and monitors external reporting from the National Monitoring Centre.

3.4 The baseline e-learning training for all officers and staff has been updated following the withdrawal of a package by the College of Policing. These are now "Managing Information" (operation and non-operational) and "Government security classification". Monitoring compliance of e-learning packages is now reported to IAB in the performance indicator report. All IAOs are still expected to complete the "Protecting Information" level 2 course and are encouraged to complete the level 3 course.

3.5 The Information Security Board has been remodelled to become the Information Assurance Board. The terms of reference, membership, standing agenda and performance indicator reports have been amended to include a wider scope of information assurance activity and decision-making regarding data protection compliance, information security assurances and records management matters. The most recent meeting held was on 18th October 2021. The next meeting is in January 2022.

3.6 Major projects continue to involve a significant amount of information security work:

i. M365 is part of the National Enabling Programme and uses Microsoft's public cloud capability. Full roll-out is now dependent on ICT capacity. It is particularly challenging for information security in terms of technical matters.

ii. Estate security and engagement with training. Infosec staff are engaged with training teams and attend induction days to provide input to both PCDA officers and new staff. A new consistent set of signage for the whole estate is in progress (in production with the supplier).

3.7 Security incidents continue to be recorded, assessed and reviewed by the ISM. Where personal information is involved, the DPO makes an assessment in relation to notifying the Information Commissioner's Office. Critical incidents are handled by "gold" groups.

4. Compliance

4.1 The Force is a registered Data Controller with the Information Commissioner's Office and is responsible for ensuring compliance with the UK GDPR and the Data Protection Act (2018) through the duties and responsibilities of the Data Protection Officer.

4.2 Remediation from the 2020 IT Security Health Check (ITHC) is incomplete due to ICT resource. This is being raised as a risk for the force's strategic risk register.

4.3 Following the 2020 IT Health Check, our "code of connection" status with the accreditors is:

(1) the Government Digital Service (GDS) who allow us to continue to connect to the Public Services Network (PSN) – our status is 'compliant/approved';

(2) the National Police Information Risk Management Team (NPIRMT) who allow our connection to the Public Service Network for Policing (PSNP) – our status is 'conditional/amber' – due to issues with ICT remediation;

(3) NPIRMT who allow our Airwave connection – our status is conditional/amber.

4.4 The new Head of Information Management and DPO was appointed in May 2021. Following appointment, they commenced a review and work is underway to refocus the activities of Information Asset Owners to identify where we use Data Processors and need data processing contracts, where we need information sharing agreements and data protection impact assessments are outstanding. The ICO's accountability self-assessment toolkit is being worked through to understand our compliance with the ICO's expectations. The findings from this toolkit will assist in identifying the full range of areas of non-compliance, documenting actions required to become compliant and assists in planning to prioritise work based on risk. Progress and risk will be reported into the Information Assurance Board.

4.5 Options are being worked through and will be documented in the Force Management Statement. The first step is understanding the scale of the issues, as described above.

4.6 A significant piece of work is underway within Records Management to understand Cleveland Police's compliance with the retention, review and deletion (RRD) of policing records and corporate paper and electronic records. Work is underway to understand any possible risks and options to remove, reduce or mitigate these risks will be presented to the Information Assurance Board.

5. Implications

5.1 Finance
There could be financial implications arising from ICO enforcement fines and civil claims brought by members of public.

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
A risk relating to the Airwave radio management has been added to the corporate risk management system.

5.6 A risk relating to the ITHC and ICT resource has been added to the corporate risk management system.

5.7 There are risks associated with non-compliance with data protection legislation including records management that may result in ICO enforcement action (including audit, being served improvement notices, recommendations and fines), risk of civil claims, risk of reputational damage and public confidence in the handling and management of personal data.

Susan Haider
Head of Information Management and Data Protection Officer
10th November 2021