Report to the Chair and Members of the Audit Committee
2 October 2020

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 2020 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), and Data Protection Officer (DPO, also the head of the Information Management Unit).

The SIRO is currently ACC Steve Graham. 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 Last year we reported a new member of staff in the role of GDPR Auditor and Deputy ISO. This auditor has carried out a large amount of work in reviewing existing and new workflows across the organisation, providing additional detail information in relation to information risks.

3.3 We are waiting for a new member of staff to start in the role of IT Security Officer (ITSO), answering to the ISM and working closely with ICT. This is to improve communications, advice and identification of risks within the ICT area. This will allow more attention to be paid to ongoing matters such as patch assurance.

3.4 The baseline training for all officers and staff remains three e-learning packages. These are "Managing Information" (operation and non-operational), "Protecting information level 1" and "Government security classification". Monitoring compliance of e-learning packages has been identified as a wider problem and referred to the People and Wellbeing Board. All IAOs are still expected to complete the "Protecting Information" level 2 course and are encouraged to consider the level 3 course.

3.5 The Information Security Board continues to meet, most recently on 25 August 2020.

3.6 Major projects involve(d) a significant information security work:

i. M365 is part of the National Enabling Programme and proposes the use of Microsoft's public cloud capability.

ii. The recently-completed ERP/DMS system update which involved moving from on-premise to Oracle's cloud infrastructure.

iii. Replacement of digital interview recorders (DIR), new body worn video (BWV) units and a new digital evidence and asset management system (DEAMS).

3.7 Security incidents continue to be recorded, assessed and reviewed by the ISM. Whether 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. Some statistics are provided in the table in the appendix.

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 Officer.

4.2 The annual IT Security Health Check (ITSHC) was conducted by an external penetration testing company in late July 2020. The report has not been received at the time of writing and is expected imminently.

4.3 Following ITSHC remediation, we will prepare and submit the Force's annual "code of connection" applications to
(1) the Government Digital Service (GDS) to continue to connect to the Public Services Network (PSN),
(2) the National Police Information Risk Management Team (NPIRMT) for our connection to the Public Service Network for Policing (PSNP), and
(3) NPIRMT for our Airwave connection.

4.4 Our current Airwave certificate is "Amber" due to poor asset management: some pool radios cannot be located and audit of handsets has revealed inconsistencies. A new attempt to locate all radios will begin in the near future, following discussion at ISB.

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
The risk of reputational harm or a breach of operational security arising from Airwave radio management has been added to the corporate risk management system.

Phil Brooke
Information Security Manager
7 September 2020

Appendix: Incident statistics

Incident type	8 Sep **2018** -7 Sep **2019**	8 Sep **2019** -7 Sep **2020**
Accidental damage/destruction	2	0
Asset misuse	0	1
Breach procedure	1	1
Cybersecurity	5	6
Disclosure	29	33
Fault	0	1
Intruder	5	1
Lost Airwave	1	9
Lost BWV	1	4
Lost ID card	26	25
Lost SIM card	1	0
Lost equipment	0	1
Lost item	2	0
Lost keys	1	0
Lost media	2	4
Lost mobile phone/device	6	10
Lost paper	3	5
Lost police equipment/uniform	5	1
Lost token	1	0
Lost warrant card	0	0
Lost/found Airwave	3	5
Lost/found BWV	1	0
Lost/found ID card	8	12
Lost/found keys	1	0
Lost/found laptop	0	1
Lost/found mobile phone/device	2	6
Lost/found paper	2	3
Physical security	9	10
Post	0	1
Stolen BWV	0	1
Stolen ID card	0	1
Stolen laptop	0	1
Suspicious incident	1	0
Unconfirmed	0	1
Unknown	0	0
Vetting	2	0
Non-incidents (cancellations, duplicates, tests)	10	5
Total	130	149