IMT Networks and Security Team

•The IMT Network and Security Team consists of 6 staff with responsibility for our IT security compliance, network infrastructure, technical security controls and Contact Centre telephony system.

•IMT currently hold the following IT Security certifications,

- •ISO 27001 – International standard for Information Security Management System
- •PCI DSS – Payment Card Industry security standard
- •PSN Certification – Public Sector Network security standard
- •IG SoC – NHS information Security Standard

•‘State of the Art’ security technologies are deployed to protect the infrastructure form the Cyber threat.

•Recent internal audit has reviewed the IT Incident management and found them adequate, appropriate, and effective.

Attack Vectors

IMT deal with a large number of cyber threats to the organisation on an ongoing basis. These include:

Email based attacks

- We process **25 million** email messages a year
- 14 million are spam (including **42,000 viruses**) identified and blocked

Internet based attacks

- **30,000 attacks** are identified and blocked each year.

Recent notable events

- Lincolnshire County Council Cyber attack (and Cyber Ransom)
- HSBC Cyber attack
- SCC Virus attack on the 2nd February where the network was bombarded viruses for a 3 hour period.

This gives you an insight into issues the IMT team deal with. We do, however, depend on all staff taking their security responsibilities seriously and being vigilant.

Security Programme - What is it?

•The security review is an update of our security policy and approach, including security training for all, introduction of new tools and techniques, more open internet access , access from home equipment and a review of supporting security technology

•In the past we have protected all of our services to the same high level of security, regardless of the sensitivity of the information they deal with. This is secure but overly restrictive. We are moving to a more personalised and risk based approach, which will support innovation and collaboration.

•IMT are trying to make our services more flexible where we can, but recognising the key risks to the organisation, improve our ability to protect the organisation and keep those who need to be secure; Secure!

Why are we doing this?

•To be able to communicate and share data with our partners.

•To respond to requests from the services to provide more internet access.

•To enable staff to use their own equipment to access IT systems, where appropriate based on the sensitivity of the data they handle, allowing them to work more flexibly.

•To maintain PSN compliance but not stifle info sharing and the use of modern technology

•To reflect the SCC Core Values – we have ‘Listened’ to the requests to review security and we are ‘Trusting’ staff to be ‘Responsible and Respectful’ with the proposed changes.

How are we making changes?

So far we have:

• Launched new ‘shorter’ IT security policy to make the information more accessible

• Launched a new Security e-learning module – available to all online

• Opened the internet to all staff to many more sites – Facebook / Twitter / You tube / Twitpic (and others) with appropriate guidance

•We have rolled out two new security products called Smoothwall and Splunk , these allow IMT staff to monitor usage easily, give access to Internet sites easily and investigate issues where needed. These are key to protecting the organisation in an ever more hostile technology world.

How are we making changes?

Future plans:

•Further opening of internet access (all sites apart from inappropriate / malicious / malware etc)

•Implement O356 which will give access to Surrey email, calendar and documents on user's personal devices.

•Review our data classification and where we store our secure and non secure data

•Allow access to more systems and data from locations outside SCC including personal devices and partner offices to support flexible and partnership working.