HENDERSON LOGGIE
Chartered Accountants

Glasgow Clyde College

IT Strategy / IT Network Arrangements

Internal Audit Report No: 2017/03

Draft Issued: 20 February 2017

Final Issued: 27 February 2017

LEVEL OF ASSURANCE	Satisfactory

Contents

		Page No.
Section 1	Overall Level of Assurance	1
Section 2	Risk Assessment	1
Section 3	Background	1
Section 4	Scope, Objectives and Overall Findings	1 - 2
Section 5	Audit Approach	3
Section 6	Summary of Main Findings	3 - 4
Section 7	Acknowledgements	4
Section 8	Findings and Action Plan	5 - 13
Appendix 1	National Cyber Security Centre 10 Steps to Cyber Security	14

Level of Assurance

In addition to the grading of individual recommendations in the action plan, audit findings are assessed and graded on an overall basis to denote the level of assurance that can be taken from the report. Risk and materiality levels are considered in the assessment and grading process as well as the general quality of the procedures in place.

Gradings are defined as follows:

Good	System meets control objectives.
Satisfactory	System meets control objectives with some weaknesses present.
Requires improvement	System has weaknesses that could prevent it achieving control objectives.
Unacceptable	System cannot meet control objectives.

Action Grades

Priority 1	Issue subjecting the College to material risk and which requires to be brought to the attention of management and the Audit Committee.
Priority 2	Issue subjecting the College to significant risk and which should be addressed by management.
Priority 3	Matters subjecting the College to minor risk or which, if addressed, will enhance efficiency and effectiveness.

1. Overall Level of Assurance

Satisfactory	System meets control objectives with some weaknesses present.

2. Risk Assessment

This review focused on the controls in place to mitigate the following risks on the College's Risk Register:

- Catastrophic failure of ICT systems / infrastructure or cyber-attack on College (net risk score: 15).

3. Background

As part of the Internal Audit programme at the Glasgow Clyde College ('the College') for 2016/17 we carried out a review of the organisation's IT strategy and IT network arrangements, including security. Our Audit Needs Assessment, finalised in March 2016, identified these as areas where risk can arise and where internal audit can assist in providing assurances to the Board and the Principal that the related control environment is operating effectively, ensuring risk is maintained at an acceptable level.

A clear Information and Communications Technology (ICT) strategy can bring significant benefits. Information technology that is appropriately matched to the College's needs will support and strengthen the College's activities and help it achieve strategic aims more efficiently and effectively.

Responsibility for ensuring an efficient and effective ICT service delivery to all staff and students within the College lies with the College's ICT Service. This includes first level support over some of the main application systems used in the provision and maintenance of user access to the network. The ICT Service is also responsible for purchasing and maintaining the servers upon which the applications are housed, the personal computers (PCs) and mobile devices used by staff and students and the network which connects them.

4. Scope, Objectives and Overall Findings

IT Network Arrangements
This aspect of the audit included a review of the College's current position with regard to Cyber Security in order to advise on areas that should be addressed in line with the latest guidance produced by the UK National Cyber Security Centre (NCSC), the UK Government's national technical authority on cyber security.

IT Strategy
This aspect of the audit included a high-level review of the College's Digital Strategy.

4. Scope, Objectives and Overall Findings (Continued)

The table below notes each separate objective for this review and records the results:

Objective	Findings			
		1	2	3
		No. of Agreed Actions		
IT Network Arrangements				
The specific objective of this aspect of the audit was to:				
1. Review the security tools in place, how these are currently used, the configuration of key elements of IT infrastructure which protect access to data, plus the policy and procedures giving guidance as to how security should be managed by both the IT department and users.	**Requires Improvement**	0	1	1
IT Strategy				
The specific objectives of this aspect of the audit were to obtain reasonable assurance that:				
2. An IT strategy group or equivalent has been formed to prepare and maintain the strategy;	**Requires Improvement**	0	1	0
3. The Digital Strategy was developed in consultation with users and taking into account the College's Development Plan and other operational plans;	**Good**	0	0	0
4. The Digital Strategy shows: ♦ objectives; ♦ how they will be achieved; ♦ resources required; ♦ clearly defined timescales for achieving specific goals and objectives; and ♦ implications;	**Good**	0	0	0
5. Staff are aware of, and have ready access to, the Digital Strategy; and	**Good**	0	0	0
6. Procedures have been established for monitoring implementation of the Digital Strategy and responsibilities formally assigned.	**Satisfactory**	0	0	0
Overall Level of Assurance	**Satisfactory**	**0**	**2**	**1**
		System meets control objectives with some weaknesses present.		

5. Audit Approach

IT Network Arrangements
Our approach was based upon the guidance and best practice provided by the NCSC; discussion with the Head of ICT and ICT Operations Manager and other members of the ICT Team, review of relevant documentation; and observation. This covered the following areas:

- Information risk management;
- Secure configuration of ICT equipment;
- Network security;
- Managing user privileges;
- ICT user education and awareness;
- Incident management;
- Malware prevention;
- Monitoring;
- Removable media controls; and
- Home and mobile working.

IT Strategy
Through discussions with the Head of ICT, and review of relevant documentation, we assessed whether the IT strategic planning process and monitoring controls accord with good practice. Applicable extracts from the Control Objectives for Information and Related Technology (COBIT) framework for information technology management and governance were used as benchmarks.

6. Summary of Main Findings

Overall, the College ICT team has a high awareness of the risks of information / cyber security, which is reflected in the control environment that demonstrates good practice in most areas. The main area of weakness is in User Education and Awareness where we found that although ICT staff demonstrated a strong awareness of information security risks the College could do more to provide information security training to expand the breadth and depth of knowledge amongst the wider staff group at all levels.

Strengths

- An appropriate risk management regime is embedded across the College, which includes identifying cyber security as key strategic risk, supported by an ICT operational risk register which identifies specific risks relating to cyber security.
- The College is a member of InfoSec, the Universities and Colleges Shared Services group for information security, which provides the College with access to information security expertise and an incident response team in the event of a significant cyber-attack.
- A baseline security build for workstations, servers, firewalls and routers is in place.
- Hardware and software inventories have been created.
- Periodic vulnerability scans are conducted of the internal network and the ICT team constantly monitors the health and activity on the IT network.
- Processes are in place for applying updates and patches to all devices connected to the College network.

6. Summary of Main Findings (continued)

Strengths (continued)

- The IT architecture protects the College network through use of firewalls and prevents direct connections to untrusted external services and protects internal IP addresses.
- Penetration testing of the external boundary is conducted annually and findings used by the ICT team to address any security weaknesses.
- Management of user accounts is linked to the College's starter, leaver and change of role procedures.
- IT Disaster Recovery plans are in place and are periodically tested.
- Network hardware is protected by an antivirus solution, which automatically scans for malware.
- Removable media is scanned for malware when connected to networked equipment.
- The College has recently started implementing a device management tool which will allow anti-virus signatures to be installed remotely on College issued laptops.

Weaknesses

- There is no overarching information security policy which clearly communicates the College's approach to information risk management.
- To be fully effective an information risk management regime should be supported by an empowered governance structure, which is actively supported by the Board and senior managers. Our review identified that there is currently no Digital Strategy Group to monitor and evaluate the implementation of the College Digital Strategy whose remit could be extended to include information risk management across the College. We have recommended that a Digital Strategy Group, comprising cross-College staff membership, is established, which has a combined responsibility for monitoring achievement of the Digital Strategy and information security considerations for IT projects.
- Our review found that although ICT staff demonstrated a strong awareness of information security risks the College is unable to demonstrate that the same level of awareness exists amongst the wider staff and user group as currently there is no structured programme of information security training provided to either staff or students.

7. Acknowledgements

We would like to take this opportunity to thank the College's ICT staff who helped us during the course of our audit.

8. Findings and Action Plan

IT Network Arrangements

Objective 1: We reviewed the security tools in place, how these are currently used, the configuration of key elements of IT infrastructure which protect access to data, plus the policy and procedures giving guidance as to how security should be managed by both the IT department and users.

The NCSC's 10 Steps to Cyber Security guidance sets out what a common cyber-attack looks like and how attackers typically undertake them. Understanding the cyber environment and adopting an approach aligned with the 10 Steps is an effective means to help protect the College from attacks.

Information Risk Management

Defining and communicating the College's Information Risk Regime should be central to the College's overall cyber security strategy. The NCSC recommends organisations review this regime – together with the nine associated security areas described in Appendix I, in order to protect against the majority of cyber-attacks.

IT Network Arrangements
Objective 1: We reviewed the security tools in place, how these are currently used, the configuration of key elements of IT infrastructure which protect access to data, plus the policy and procedures giving guidance as to how security should be managed by both the IT department and users (continued).

Observation	Risk	Recommendation	Management Response
At a corporate level an appropriate risk management regime is embedded across the College with a strategic risk register, which identifies cyber security as a key risk, and operational risk registers in place, which are monitored by the Audit Committee and management. This includes an ICT risk register which specifically identifies cyber security risks. However, there is no overarching information security policy which clearly communicates the College's approach to information risk management. The College is a member of InfoSec, the Universities and Colleges Shared Services group for information security. The Chief Information Security Officer of InfoSec recently presented to the College Senior Management Team on cyber security issues.	Employees, students, contractors and suppliers are not aware of the College's approach to information risk management.	**R1** Develop an Information Risk Management Policy, which is approved and supported by the Board of Management, which clearly communicates the College's approach to information risk management. This should aim to ensure that all employees, students, contractors and suppliers are aware of the College's approach, how decisions are made, and any applicable risk boundaries.	As part of the InfoSec membership, the College will undertake a Business Impact Analysis. This includes a five-step process which will undertake a review of current Information controls and conclude with a Risk Report. Based on the outcome of this exercise, the College will develop and adopt an Information Risk Management Policy. **To be actioned by:** VP Resources & AP Finance & Infrastructure **No later than:** September 2017
			Grade 3

Objective 1: We reviewed the security tools in place, how these are currently used, the configuration of key elements of IT infrastructure which protect access to data, plus the policy and procedures giving guidance as to how security should be managed by both the IT department and users (continued).

To be fully effective an information risk management regime should be supported by an empowered governance structure, which is actively supported by the Board and senior managers. Our review identified that there is no Digital Strategy Group, in place which would act as an appropriate body for evaluating and monitoring IT projects, including monitoring information security risks as they arise during the implementation of the College's Digital Strategy.

Without IT articulating information security risks, in a format that senior management understands, and ensuring it is presented at the correct forum, it will be difficult for the College to make risk based decisions and provide the appropriate resources to align IT security capability with the organisational risk appetite. We have recommended at **R3** that the College considers establishing a Digital Strategy Group whose remit would be to review procedures relating to information security.

Objective 1: We reviewed the security tools in place, how these are currently used, the configuration of key elements of IT infrastructure which protect access to data, plus the policy and procedures giving guidance as to how security should be managed by both the IT department and users (continued).

Having an approach to identify baseline technology builds and processes for ensuring configuration management can greatly improve the security of systems. Developing a strategy to remove or disable unnecessary functionality from systems, and to quickly fix known vulnerabilities, usually via patching can reduce the risk of compromise of systems and information. Our review noted that, overall, the College has robust information security controls in place, including:

- polices to update and patch systems that set out the priority and timescales for applying updates and patches;
- hardware and software inventories have been created;
- servers and workstations, where possible, are standardised with uniform specifications which include standard security settings;
- the health of the IT network is monitored regularly by ICT staff; and
- penetration testing of the IT network boundary is undertaken annually by an external agency and findings are used to address any security weaknesses.

The latest penetration testing conducted in the summer of 2016 identified 19 high grade risks which related to four specific issues, including:

- PHP, a general-purpose scripting language which runs on a web server, was out of date and therefore unsupported meaning that security patches are no longer automatically provided for any new security vulnerabilities;
- a Microsoft Windows 2003 server installed on the network which is no longer supported;
- versions of OpenSSL/H, tools used to encrypt communications across computer networks, were out of date; and
- the Cisco ASA, which provides a network defence through a combination of firewalls, antivirus and intrusion prevention, was out of date.

Following the last penetration test an action plan was developed to address the identified weaknesses. At the time of our review we noted that the high level risks had either been addressed or that updates or maintenance had been scheduled to resolve the issues. We also found that the majority of medium and low grade risks had been addressed.

A number of vulnerabilities were also identified and these are detailed below under the relevant NCSC 10 Steps to Cyber Security headings as outlined in Appendix 1.

Objective 1: We reviewed the security tools in place, how these are currently used, the configuration of key elements of IT infrastructure which protect access to data, plus the policy and procedures giving guidance as to how security should be managed by both the IT department and users (continued).

Secure Configuration

At the time of our review we found that 80% of the College's network hardware was covered by the anti-virus solution, of which the latest anti-virus signature had been applied to 60% of networked IT equipment. Equipment not covered by the latest ant-virus includes a number of laptops that are issued to staff and which may not be plugged into the College network for several weeks at a time, and the College also owns a bank of computers used in classrooms some of which can remain unused all year. However, procedures are in place whereby ICT staff ensure that all classroom laptops are updated annually during the summer break. As anti-virus is automatically updated on IT hardware when connected to the College network we are satisfied that the risks are adequately mitigated.

To ensure that anti-virus is installed on laptops issued to staff, the College has recently purchased and is currently implementing a Device Management application (SNOW) which will allow the ICT team to monitor and manage remote devices.

Laptops currently deployed by the College (Microsoft Surface Pro) are not encrypted. The ICT team has identified this as a risk on the ICT operational risk register and we understand that a suitable encryption solution will be applied to mobile devices with the implementation of Windows 10 later in 2017.

Removable Media Controls

The use of removable media such as USBs and DVDs media is currently unrestricted and there is no requirement to ensure that only encrypted USBs are used. In order to reduce the risk of data loss the ICT team has encouraged staff to use Office 365 and SharePoint which has stronger document management controls. However this does not reduce the risk of viruses being introduced into the College network from removable media. We acknowledge the flexibility required by both staff and students for using USBs and so to mitigate the risks associated with this policy the College has put additional controls in place, including anti-virus installed across the network, and disabling the Auto Run function on removable media. Providing encrypted USBs to staff is currently being considered by ICT.

Objective 1: We reviewed the security tools in place, how these are currently used, the configuration of key elements of IT infrastructure which protect access to data, plus the policy and procedures giving guidance as to how security should be managed by both the IT department and users (continued).

Managing User Privileges

The ICT team consists of 10 staff that have been assigned IT network administrator privileges. Our review noted that in order to allow operational flexibility administrators do not have separate user accounts for administrator duties and day-to-day activities such as email and internet. Per discussions with the Head of ICT, the College has considered the use of separate accounts for privileged level access but found this to be an unnecessary barrier for the team to carry out their daily tasks as it would decrease efficiency. Alternative controls are in place which include: the room in which IT Network Administrators are based is always manned; the College has password policies in place to protect accounts; and the network is constantly monitored for any unusual activity. However, good practice recommends that separate accounts are used to reduce the risk of network security being compromised and this should be kept under review by the College.

User Education and Awareness

Users have a critical role to play in the College's security and so it's important that security rules and the technology provided enables users to do their job as well as help keep the College secure. This can be supported by a systematic delivery of awareness programmes and training that deliver security expertise as well as helping to establish a security-conscious culture.

Objective 1: We reviewed the security tools in place, how these are currently used, the configuration of key elements of IT infrastructure which protect access to data, plus the policy and procedures giving guidance as to how security should be managed by both the IT department and users (continued).

Observation	Risk	Recommendation	Management Response
Our review found that although ICT staff demonstrated a strong awareness of information security risks the College is unable to demonstrate that the same level of awareness exists amongst the wider staff and user group as currently there is no structured programme of information security training provided to either staff or students. Acceptable use of the College's IT systems is covered by online learning modules as part of the new staff induction process. Both staff and students are required to agree to the Colleges Acceptable Use Policy (AUP) by way of an on-screen dialogue box at log-in which sign posts users to, but does not require that the user reads, the AUP. However, we also noted that staff are only required to agree to the AUP at point of first log-in only. A key element of the College Development Plan is leveraging the use of technology in the delivery of learning and teaching and in improving the efficiency of business processes. Therefore it is vital that staff are provided with adequate information security training to mitigate the risk of malicious or accidental data loss resulting from an increased use of technology.	Organisations that do not effectively support employees through education and awareness may be vulnerable to a range of risks, including: • introduction of malware and data loss through use of removable media; • legal sanctions due to loss of sensitive data; • external attacks due to email phishing and social engineering; and • data loss or corruption due to an internal attack by a dissatisfied employee.	**R2** Develop a programme of information security training for new and existing users to mitigate information security risks, covering: • the College's information security policy (see **R1**); • an induction process for new users (including contractors and third party users); • regular refresher training on the security risks to the College; • supporting staff in information security roles to enrol on a recognised certification scheme; • monitoring the effectiveness of security training; • promoting an incident reporting culture; and • establishing a formal disciplinary process to address abuse of the College's security policies.	As part of the College's Infosec membership, training material on Information Security is being developed for distribution. The College already has in place an Acceptable Use Agreement for staff which would be enforceable by College disciplinary procedures. As part of the InfoSec membership a FE / HE cross-sector CIRT (Computer Incident Response Team) is being created. **To be actioned by:** Senior Management Team **No later than:** September 2017 **Grade** 2

IT Strategy

Objectives 2 - 6 :

- **an IT strategy group or equivalent has been formed to prepare and maintain the strategy;**
- **the Digital Strategy was developed in consultation with users and taking into account the College's Development Plan and other operational plans;**
- **the Digital Strategy shows:**
  - **objectives;**
  - **how they will be achieved;**
  - **resources required;**
  - **clearly defined timescales for achieving specific goals and objectives; and**
  - **implications;**
- **staff are aware of, and have ready access to, the Digital Strategy; and**
- **procedures have been established for monitoring implementation of the Digital Strategy and responsibilities formally assigned.**

The College has developed a Digital Strategy 2016-2020 which sets out a framework for the College's use of digital technologies to support the business objectives of the College. A supporting Action Plan has also been produced which includes a number of actions linked to the College Development Plan which are grouped under the headings of Staff Development, Improved Infrastructure, Unified Communications, Business Systems Developments and Key Performance Measures. The Digital Strategy and Action Plan are monitored by the Head of ICT, the Assistant Principal, Finance and Infrastructure and the Vice Principal, Resources and College Development.

IT user forums have been established at each campus which are attended by ICT staff but chaired by curriculum staff. Feedback from these forums, including staff views on systems, applications and process improvements, were considered during the development of the Digital Strategy and also the IT Road Map.

Given the rate at which technology changes the actual costs, equipment and timescales required to achieve the objectives of the Digital Strategy may decrease or increase over time and therefore the resources and timescales have not been included within the Strategy. Key Performance Measures are to be in place by the end of the current academic year which will be used to measure the impact of the Digital Strategy Action Plan.

The Digital Strategy is available to all staff on the staff portal.

It is anticipated that the Digital Strategy will be reviewed on an annual basis by the SMT and any necessary changes to the original solutions proposed in the Strategy will be taken into account.

IT Strategy

Objectives 2 - 6 (continued):

Observation	Risk	Recommendation	Management Response
An ICT / Digital Strategy Group is not currently in place which comprises cross-College membership including representatives from academic staff, support staff, ICT staff, students, Estates and members of the SMT. A formal remit for the Digital Strategy Group should be approved which defines the role of the group, for example, to develop, monitor and evaluate the implementation of the College Digital Strategy. The Group should meet regularly throughout the year with agendas set for each meeting and minutes documented and made available on the staff intranet. Sub-groups of the Digital Strategy Group should also be developed in line with the headings of the Digital Strategy Action Plan and the strategic aims outlined in the Digital Strategy, which include: Staff Development, Improved Infrastructure, Unified Communications and Business Systems Developments. The purpose of each of the above groups would be to review aspects of the Digital Strategy which impact each group. Findings should then be reported to the main Digital Strategy Group.	ICT tasks / projects are not subject to an adequate governance approach which includes engagement from all stakeholders including business owners and users across the College.	**R3** Consider establishing a Digital Strategy Group (or equivalent) which comprises cross College staff representation to act as an appropriate body for evaluating and monitoring IT projects and implementation of the Digital Strategy. Formalise the remit of the group, ensuring that the group: • monitors the Digital Strategy, ensuring that it conforms to and supports the strategic priorities of the College; • considers initiatives and innovations in use more widely across the College; and • approves IT policies and procedures relating to information security.	The College has recently set up a College Wide Improvement Group with cross College representation. This group will evaluate and monitor IT projects and the implementation of the Digital Strategy Action Plan and will consider feedback from the IT users' forums. There will be the option of short life working groups (rather than sub groups) on specific elements as appropriate. **To be actioned by:** VP Resources & College Development **No later than:** June 2017 **Grade** **2**

National Cyber Security Centre

10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention

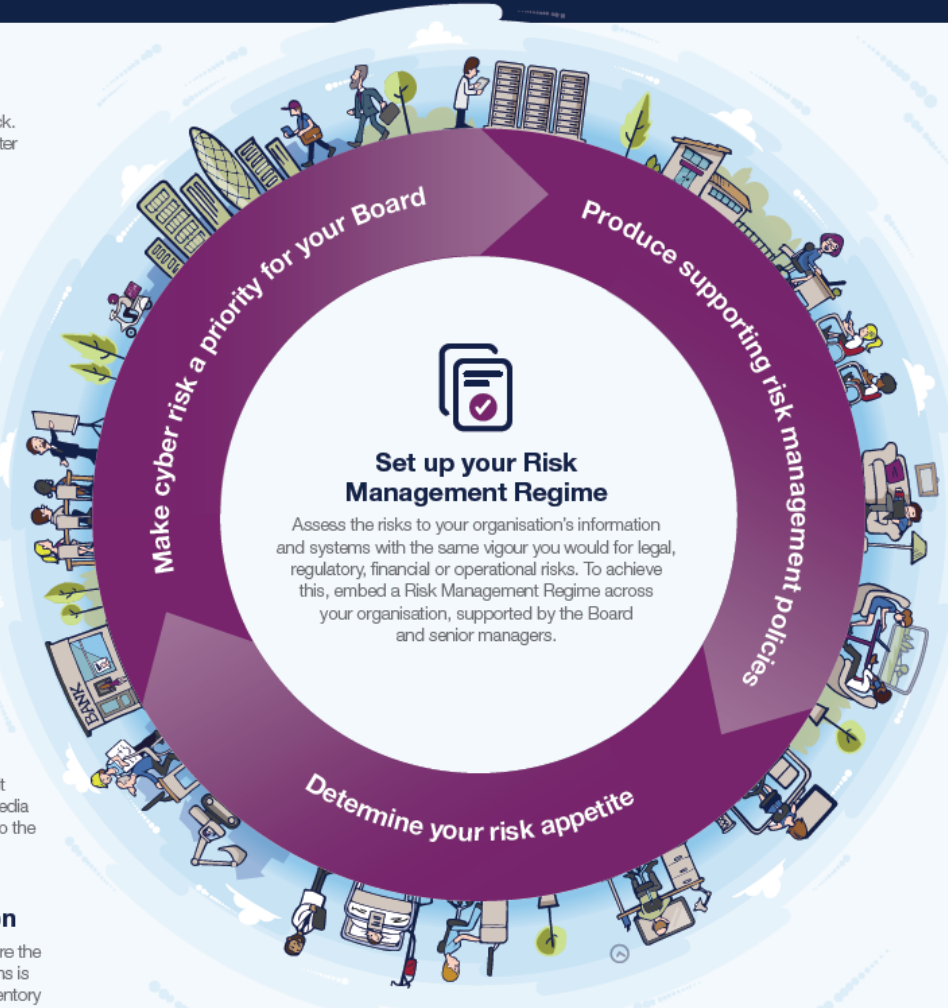
Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.



Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to www.ncsc.gov.uk @ncsc