

# NEN – The Education Network



## School e-Security Checklist

### November 2014

This checklist sets out 20 e-security controls that, if implemented effectively, will help to ensure that school networks are kept secure and protected from internal and external threats.

The advice presented here is adapted from the Council on Cyber Security's *Critical Security Controls* document<sup>1</sup>. The description of each control is accompanied by two sets of questions: one for school network managers and support staff, and one for school head teachers and senior leadership teams. The former are concerned with operational matters, while the latter focus on policy, strategy and budgetary considerations.

While the majority if not all of these controls need to be in place to keep school networks secure and protected, clearly implementing and maintaining the 20 controls described here is a very significant undertaking. It is anticipated that while some of these controls are best implemented and managed in-house, others may be provided by third parties. These might include organisations providing broadband and wide area network services, such as local authorities, regional broadband consortia (RBCs) and/or commercial broadband providers. Some controls might be provided by third parties other than broadband providers, such as commercial ICT support and managed service providers. Schools can use this document to review and record their existing e-security arrangements (in particular, to identify which controls are provided in house and which are provided by third parties). Schools may also wish to use this document to evaluate the service offerings of any providers they may be considering using in the future.

An accompanying document, *e-Security – 10 steps to protect your school's network*, provides a one page overview of these controls for school senior leadership teams.

Further advice is available in *NEN Information Sheet 6: e-Security – Managing and maintaining e-security/cyber-security in schools*. Both are available on the NEN website at <http://www.nen.gov.uk>.

---

<sup>1</sup> <http://www.counciloncybersecurity.org/critical-controls/>

Critical Security Control	Questions for School Network Managers & Technicians	Questions for School Head Teachers, Senior Leaders and Governors	Done in-house	Done by broadband service provider	Done by another service provider
<p><b>CSC 1: Inventory of Authorized and Unauthorized Devices:</b> Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.</p>	<ul style="list-style-type: none"> <li>Do you have a detailed, up to date list of all network hardware and devices on your network?</li> <li>Do you have processes in place to regularly review and update this?</li> <li>Do you have mechanisms and/or processes in place to detect when/if any unauthorised devices are connected to your network, and to prevent any such devices from gaining access to data and facilities?</li> </ul>	<ul style="list-style-type: none"> <li>Does your school's IT acceptable use policy (AUP) include provisions/instructions to ensure only authorised devices are connected to the school's network?</li> </ul>			
<p><b>CSC 2: Inventory of Authorized and Unauthorized Software:</b> Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.</p>	<ul style="list-style-type: none"> <li>Do you have a detailed, up to date list of all software used in school?</li> <li>Do you have processes in place to regularly review and update this as necessary?</li> <li>Do you have mechanisms and/or processes in place to detect when/if any unauthorised software is installed on the network, and to prevent any such software from being used?</li> </ul>	<ul style="list-style-type: none"> <li>Does your school's IT acceptable use policy (AUP) include provisions/instructions to ensure only authorised software is used in school?</li> </ul>			
<p><b>CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers:</b> Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.</p>	<ul style="list-style-type: none"> <li>Do you have standard secure configurations for the operating systems and applications used in school, together with processes to ensure these are consistently applied and maintained (for example, re-imaging with secure builds if any system becomes compromised)?</li> <li>Do you have patching tools and processes to update hardware and software promptly?</li> <li>Are administrative privileges appropriately allocated and limited?</li> <li>Do you have details of the lifecycles of all your software and hardware – do you know when manufacturers' support for hardware and software will end, and what will you do when it does?</li> </ul>	<ul style="list-style-type: none"> <li>Does your school's IT acceptable use policy (AUP) include clear provisions/instructions warning users about tampering with secure configurations, with clear sanctions for any infraction?</li> <li>Do you have visibility of likely costs to upgrade and refresh hardware and software as necessary, and when these costs are likely to be incurred (for example, antivirus software subscriptions, firewall support and maintenance services, dates for when hardware/software will go "end of life" and need to be replaced)?</li> </ul>			

Critical Security Control	Questions for School Network Managers & Technicians	Questions for School Head Teachers, Senior Leaders and Governors	Done in-house	Done by broadband service provider	Done by another service provider
<p><b>CSC 4: Continuous Vulnerability Assessment and Remediation:</b> Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.</p>	<ul style="list-style-type: none"> <li>How do you ensure you keep abreast of new and emerging risks and issues, reviewing and updating your e-security processes, software and hardware accordingly?</li> <li>How do you ensure updates and patches are applied in a timely fashion once vulnerabilities have been identified?</li> </ul>	<ul style="list-style-type: none"> <li>Do you have processes in place for regular review of e-security functions and your IT acceptable use policies to address new and emerging threats?</li> <li>How do you ensure staff and pupils receive appropriate e-security advice and training?</li> </ul>			
<p><b>CSC 5: Malware Defences:</b> Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defence, data gathering, and corrective action.</p>	<ul style="list-style-type: none"> <li>How do you prevent malware across your school's network?</li> <li>How regularly do you check that no malware is present?</li> <li>How do you ensure that anti-malware software is kept up to date?</li> <li>What steps do you take to ensure that malware risks from removable media like USB flash drives are minimised?</li> </ul>	<ul style="list-style-type: none"> <li>How do you ensure that your user education processes and IT acceptable use policies are up to date to minimise risks in this area?</li> <li>What sanctions are applied for malicious use of school IT services and systems?</li> </ul>			
<p><b>CSC 6: Application Software Security:</b> Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect and correct security weaknesses</p>	<ul style="list-style-type: none"> <li>How do you ensure that you are using the most up to date versions of software?</li> <li>Do you know when manufacturer support for the software you are currently using will end? What will you do when it does?</li> <li>What e-security track record does the vendor of any new software you are considering have?</li> </ul>	<ul style="list-style-type: none"> <li>Do you have visibility of when significant upgrade and renewal of software will be required, both in terms of likely cost and ensuring service continuity?</li> <li>How do you ensure staff and pupils are trained in the use of new software?</li> </ul>			
<p><b>CSC 7: Wireless Access Control:</b> The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.</p>	<ul style="list-style-type: none"> <li>How do you ensure only authorised devices can connect to your school's wireless network?</li> <li>How do you manage and maintain security for devices which are used both in and away from school? (for example, staff laptops and/or pupil-owned devices if a bring your own device policy is in place – how is access provided to untrusted devices, if this is required?)</li> <li>How do you ensure services and systems are kept secure if guest access or BYOD options are provided?</li> </ul>	<ul style="list-style-type: none"> <li>What is the school's policy on wireless access – do you allow guest access, or access from staff- or pupil-owned devices?</li> <li>Does your IT AUP appropriately encompass access from staff- or pupil-owned devices if this is allowed?</li> <li>Do your staff and pupils understand their obligations and responsibilities in relation to using their own devices in school, if they are allowed to do so?</li> </ul>			

Critical Security Control	Questions for School Network Managers & Technicians	Questions for School Head Teachers, Senior Leaders and Governors	Done in-house	Done by broadband service provider	Done by another service provider
<p><b>CSC 8: Data Recovery Capability:</b> The processes and tools used to back up critical information properly with a proven methodology for timely recovery.</p>	<ul style="list-style-type: none"> <li>Do you have process in place for backing up school data securely and restoring it in the event of a security incident?</li> <li>How regularly are backups made?</li> <li>Where are backups stored and how secure are your storage arrangements?</li> <li>How quickly could you restore critical school data from a backup if you needed to do so?</li> </ul>	<ul style="list-style-type: none"> <li>Does your school have an overarching disaster recovery/business continuity plan?</li> <li>If so, does this encompass restoration of IT facilities and critical school data appropriately?</li> </ul>			
<p><b>CSC 9: Security Skills Assessment and Appropriate Training to Fill Gaps:</b> For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defence of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.</p>	<ul style="list-style-type: none"> <li>Do you have an understanding of the skills, abilities and training needs of all members of your team?</li> <li>How do you keep up to date with new and emerging security threats?</li> </ul>	<ul style="list-style-type: none"> <li>Does your school's overarching staff training and development planning include provisions to ensure that technical support staff can keep up to date with e-security risks and best practices and that all teaching and administrative personnel understand their own e-security obligations and responsibilities?</li> </ul>			
<p><b>CSC 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches:</b> Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.</p>	<ul style="list-style-type: none"> <li>Do you have policies and processes for ensuring and maintain secure configurations for all network devices such as firewalls, routers and switches?</li> <li>How do you securely manage and implement any necessary changes to these devices and ensure they are kept up to date?</li> <li>If support is provided by a third party, how would you maintain security if the third party were to discontinue its services for any reason?</li> </ul>	<ul style="list-style-type: none"> <li>Do you have visibility/awareness of when major changes and/or upgrades will need to be carried out, in terms of both likely cost/budgeting and maintaining service continuity?</li> </ul>			
<p><b>CSC 11: Limitation and Control of Network Ports, Protocols, and Services:</b> Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.</p>	<ul style="list-style-type: none"> <li>How do you ensure that only the necessary ports, protocols, and services are running on each system?</li> <li>How do you manage and maintain your firewall(s) to ensure it/they is/are secure, up to date and supporting the needs of the school?</li> </ul>	<ul style="list-style-type: none"> <li>Do you have visibility of when major changes are likely to be necessary?</li> <li>Do you have effective processes for communicating changes, for example in relation to changing security settings to allow access to a new service or facility – are appropriate risk assessment and management processes in place and adhered to?</li> </ul>			

Critical Security Control	Questions for School Network Managers & Technicians	Questions for School Head Teachers, Senior Leaders and Governors	Done in-house	Done by broadband service provider	Done by another service provider
<p><b>CSC 12: Controlled Use of Administrative Privileges:</b> The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.</p>	<ul style="list-style-type: none"> <li>• How do you ensure administrative privileges are allocated appropriately?</li> <li>• Do you have complex password requirements for all administrator accounts?</li> <li>• How do you ensure that all default passwords are changed?</li> </ul>	<ul style="list-style-type: none"> <li>• Do you have effective user education strategies in place to ensure the importance of administrator privileges and understood and respected?</li> <li>• Does your IT acceptable use policy require strong, complex passwords and regular password changes?</li> </ul>			
<p><b>CSC 13: Boundary Defence:</b> Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.</p>	<ul style="list-style-type: none"> <li>• Are your boundary defences multi-layered? (for example, encompassing firewalls, proxies, DMZ perimeter networks, network-based intrusion detection and prevention)</li> <li>• Do you maintain any blacklists of known malicious sites, or whitelists of trusted sites?</li> <li>• How do you provide secure remote access to your network, if required?</li> </ul>	<ul style="list-style-type: none"> <li>• How regularly are your boundary defences reviewed and tested?</li> <li>• Do you employ any independent third party testing of your boundary defences to maintain their effectiveness in the light of dynamic and emerging threats?</li> </ul>			
<p><b>CSC 14: Maintenance, Monitoring, and Analysis of Audit Logs:</b> Collect, manage, and analyse audit logs of events that could help detect, understand, or recover from an attack.</p>	<ul style="list-style-type: none"> <li>• Do you keep and review sufficient log information to be able to detect, recover and learn from a security incident?</li> <li>• How do you ensure you have sufficient storage arrangements for monitoring and logging data, for example to provide evidence in relation to an as yet undiscovered security incident?</li> </ul>	<ul style="list-style-type: none"> <li>• How do you ensure that sufficient time is allocated to reviewing and acting upon the outputs from monitoring and logging activities?</li> <li>• Where do responsibilities for reviewing outputs from monitoring and logging reside?</li> <li>• What are your data retention policies, and where are they described?</li> </ul>			
<p><b>CSC 15: Controlled Access Based on the Need to Know:</b> The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.</p>	<ul style="list-style-type: none"> <li>• How do you differentiate access by user group (staff, pupils, IT support personnel)?</li> <li>• How do you limit access to services and sensitive data on your network only to authorised users?</li> </ul>	<ul style="list-style-type: none"> <li>• Does your IT acceptable use policy differentiate between the obligations and responsibilities of different groups of users (teaching staff, administrative/managerial staff, pupils, governors)?</li> <li>• How do you communicate with and keep different user groups up to date with their obligations and responsibilities?</li> </ul>			

Critical Security Control	Questions for School Network Managers & Technicians	Questions for School Head Teachers, Senior Leaders and Governors	Done in-house	Done by broadband service provider	Done by another service provider
<p><b>CSC 16: Account Monitoring and Control:</b> Actively manage the life-cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.</p>	<ul style="list-style-type: none"> <li>• What processes are employed for provisioning, managing, monitoring and deleting user accounts as required?</li> <li>• How often is the list of current user accounts reviewed?</li> <li>• Do you employ an expiration date for inactive/dormant accounts?</li> <li>• Are users required to lock screens when leaving devices temporarily unattended?</li> <li>• Is a strong password policy requiring regular new passwords in place and enforced?</li> <li>• Do you undertake any monitoring of user accounts for unusual usage?</li> </ul>	<ul style="list-style-type: none"> <li>• How do you communicate with, educate and inform different user groups of their obligations and responsibilities?</li> <li>• How regularly is your IT AUP updated in the light of new threats and lessons learned from previous incidents?</li> </ul>			
<p><b>CSC 17: Data Protection:</b> The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information (exfiltration: the unauthorized release of data from within a computer system or network)</p>	<ul style="list-style-type: none"> <li>• Do you encrypt all sensitive data?</li> <li>• Do you know where all your schools' data is held – in school, in private clouds, the public cloud?</li> <li>• For data held in the cloud, do you have a strategy for switching cloud provider if required, or for ensuring that all your schools' data can be extracted from the service if required?</li> <li>• Do you have processes and policies in place to prevent theft or loss of devices – for example, can sensitive data be written to unencrypted USB flash drives for removal from school premises?</li> </ul>	<ul style="list-style-type: none"> <li>• Are all staff and pupils aware of all their responsibilities and obligations in relation to sensitive and personal data, particularly in the light of schools' roles as data controllers under The Data Protection Act 1998?</li> </ul>			
<p><b>CSC 18: Incident Response and Management:</b> Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.</p>	<ul style="list-style-type: none"> <li>• Do have defined processes for responding to and managing security incidents?</li> <li>• Are the roles and duties of key individuals sufficiently defined to ensure effective action is taken quickly in the event of a security incident?</li> <li>• Are logs and records kept for all incidents?</li> </ul>	<ul style="list-style-type: none"> <li>• How regularly are incident handling processes reviewed?</li> <li>• Do you undertaken any example incident scenarios to test and update incident handling processes and procedures?</li> </ul>			

Critical Security Control	Questions for School Network Managers & Technicians	Questions for School Head Teachers, Senior Leaders and Governors	Done in-house	Done by broadband service provider	Done by another service provider
<p><b>CSC 19: Secure Network Engineering:</b> Make security an inherent attribute of the enterprise by specifying, designing, and building---in features that allow high confidence systems operations while denying or minimizing opportunities for attackers.</p>	<ul style="list-style-type: none"> <li>• How regularly do you review your whole network infrastructure, policies and procedures in the light of new security technologies and techniques and emerging risks and issues?</li> <li>• How easy is it to make changes to update and improve security protections?</li> <li>• Do you employ any third parties to review your infrastructure, policies and procedures and suggest improvements?</li> </ul>	<ul style="list-style-type: none"> <li>• How much and how often are time and resources allocated to reviewing and updating the school network as a whole?</li> <li>• What processes and analysis are employed to determine which security functions are best provided in house and which should be delivered using the expertise of third parties such as broadband service providers?</li> </ul>			
<p><b>CSC 20: Penetration Tests and Red Team Exercises:</b> Test the overall strength of an organization’s defences (the technology, the processes, and the people) by simulating the objectives and actions of an attacker</p>	<ul style="list-style-type: none"> <li>• Do you conduct any internal or external penetration testing of your schools’ network?</li> <li>• How do you respond and learn from the results from such exercises?</li> </ul>	<ul style="list-style-type: none"> <li>• How do you identify sources of advice and support that can scrutinise the security of you network and suggest an action plan for improvement?</li> </ul>			