

# AUDIT COMMITTEE REPORT

<b>Subject:</b> Cyber Security Update	<b>Purpose:</b> <b>For Approval</b> <input type="checkbox"/> <b>For Discussion</b> <input type="checkbox"/> <b>For Information</b> <input checked="" type="checkbox"/>	
<b>Prepared by:</b> Scott Moncrieff, Head of ISLT Kirsty Robb – VP Finance & Corporate Services	<b>Date:</b> 24 November 2022	
<b>Purpose:</b> To provide Audit Committee with an update regarding College Cybersecurity enhancements.		
<b>Linked to Strategic Ambition:</b> Create high quality learning and training opportunities which are relevant, enabling and flexible		
<b>Performance Measures:</b> Delivery models are personalised focusing on individual & business need		
<b>Linked to Strategic Risk Register:</b> 3a - Information Management		
<b>New Risk Commentary:</b>		
<b>Executive Summary:</b>  The provision of a high quality, technically resilient ICT infrastructure is an essential component to support the College in securing its systems and data and ultimately enabling a high quality learning experience.  In recent years substantial steps have been to enhance our cybersecurity and the below report provides the Committee with an update in relation to some of the work undertaken in recent months to further enhance our network and data.  In the period since the previous update work has concentrated on operational work, and the key areas listed below, with full detail given in appendix A..  <ul style="list-style-type: none"> <li>• Jisc Security Conference</li> <li>• Cyber Essentials Plus</li> <li>• Operational Work</li> </ul>		
<b>Recommendation:</b> Members are asked to review the paper which reflects continuing progress on cyber security.		
<b>Previous Committee Approvals:</b> none		
<b>For publication</b> <input checked="" type="checkbox"/>	<b>For publication with redactions</b> <input type="checkbox"/>	<b>Not for publication</b> <input type="checkbox"/>

## **Jisc Security Conference 2022**

Jisc is the UK digital, data and technology agency focused on tertiary education, research and innovation. Borders College along with the vast majority of education institutions are members of Jisc. Jisc provide the JANET Internet connection as well as many security services which wraparound this to help protect our network. They also offer many other services to assist HE/FE, more information on JISC can be found here – [www.jisc.ac.uk/about](http://www.jisc.ac.uk/about)

Our Infrastructure Technician and Head of ISLT attended the recent Jisc Security Conference at the ICC in Wales.

The event was attended by over 300 staff from the HE/FE sector and concentrated on what Jisc are doing to improve the security of the JANET network, what threats are common within the sector as well as what mitigations are currently available to us and future developments are in the pipeline.

A number of the talks were around the challenges which face the sector in achieving Cyber Essentials Plus due to the new criteria which has been introduced which are detailed further below.

Other workshops and talks were around experiences of Cyber-attacks and lessons learnt on sharing information, as well as products designed to assist with the prevention and recovery processes of Cyber threats.

A lot of follow up discussions were arranged with JISC to discuss various solutions such as

- Ransomware awareness and scenario based training
- Advanced security solutions
- SIEM service offering – This assists with 24/7/365 monitoring of our network in relation to cyber attacks
- Collaboration with other FE/HE institutions on similar work we are carrying out to learn from each other

## **Cyber Essentials Plus**

The Scottish Government advises all Public Sector organisations to achieve Cyber Essentials and Cyber Essentials Plus accreditations in order to evidence a baseline level of security. The higher level Cyber Essential Plus has the additional requirement of a hands-on technical verification.

Over the past 3 years we have successfully gained our Cyber Essentials Plus accreditation, our date for renewal is the end of January 2023.

The criteria for successful accreditation changed due to felt the change in working practices and the move to a more hybrid practices. This has caused major concern within the sector recently due to the additional work required to achieve this.

The major changes relate to mobile devices such as staff mobile phones as well as

students who use their own devices. This is known as Bring Your Own Device (BYOD)

Clarity is currently being sort around elements of BYOD as it's argued students don't connect to the corporate network, they connect to the Eduroam WiFi network and only access Microsoft 365 and Canvas course material, not corporate data. Eduroam is the secure, world-wide roaming access service developed for the international research and education community available in the majority of education institutions worldwide.

Mobile device management requires more work and potentially investment in a management solution in which it can manage not only college provided mobile phones but also the data on staffs personal mobile phones if they use these for Email, Teams etc.

Another area of concern is staff laptops. The current a rolling replacement programme of staff laptops over 4 years old has been delayed. The programme ensured the devices are of adequate technical specification to allow the staff member to perform their role efficiently and not be affected by a poorly performing laptop. This also allowed ensured the Windows 10 operating system is always supported as Windows 10 has many versions which go out of support after a period of time.

However the budget for this year's replacements was removed meaning these laptops will remain in circulation.

The budget for replacement s was removed for 2022/23 which has resulted in around 60 devices being or will soon to be on a unsupported version of Windows 10. This would be a fail for CE+. There is a plan to start upgrading these, however may take until summer 2023 due to less resources available within the IT team.

The risk of all this is that we may be unable to achieve CE+ in January and successful accreditation might not happen until later nearer the summer of 2023. Currently for a college there is no perceived risk for not achieving Cyber Essentials, however some funding requests 'may' as for CE/CE+ as a condition of award.

## Operational Enhancements

Below are some of the operational actions we have taken recently to ensure our network stays safe.

Action	Benefit
<b>Vulnerability scanning</b>	We run vulnerability scans on our servers each week to identify potential issues and perform appropriate work to resolve these.
<b>PingCastle software</b>	As well as our vulnerability scanning we have started using a solution called PingCastle which scans our Active Directory for vulnerabilities.  The team are just getting used this software and an update to the findings will be provide at the next Audit Committee meeting.

<b>New VPN Client</b>	<p>Preparation and testing of a new VPN client for staff is ongoing. This new version will enhance security and is planned to be rolled out in January.</p> <p>VPN is the solution which provides staff access our secure network when working remotely.</p>
<b>Jisc 16 Question Cyber Survey</b>	<p>In the paper present to Audit Committee in May 2022, it was outlined where we are in relation to the JISC 16 questions Cyber survey, work continues on this and an update will be provided at the next Audit Committee meeting.</p>