F

AUDIT COMMITTEE REPORT

Subject: Cyber Security Update	**Purpose:** **For Approval** ☐ **For Discussion** ☐ **For Information** ☒
Prepared by: Scott Moncrieff, Head of ISLT	**Date:** 20 January 2022

Purpose: To provide Audit Committee with an update regarding College Cybersecurity enhancements.

Linked to Strategic Ambition: Create high quality learning and training opportunities which are relevant, enabling and flexible

Performance Measures: Delivery models are personalised focusing on individual & business need

Linked to Strategic Risk Register: 3a - Information Management

New Risk Commentary:

Executive Summary:

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 we have taken substantial steps 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.

These updates below provide information on

- Cyber Essentials Plus Accreditation
- Office 365 backups
- Disaster Recovery Testing
- Cyber Insurance
- VPN
- IT Audit

Recommendation: Members are asked to review the paper which reflects continuing progress on cyber security.

Previous Committee Approvals:
none

For publication ☒	**For publication with redactions** ☐	**Not for publication** ☐

Cyber Essentials / CE+

In November we successfully achieved the first part of our Cyber Essentials accreditation for 2021/22, this has involved completing in excess of 50 questions based on our network, security and processes.

The next stage of gaining Cyber Essentials+ accreditation which includes working with our security partner Barrier Networks and providing evidence on a selection of the questions is almost complete.

We had planned to complete this by Christmas however due to resource issues (Covid) at Barrier Networks we agreed to move this to January.

Once completed and passed this demonstrates we are at the minimum level set out by the government for Cyber protection. With the work we have completed in recent years on our protection we are confident that we not only meet that level, but in many areas, exceed it.

Having accreditation demonstrates to students, partners and any potential businesses that we take Cyber Security and the data of our staff and students seriously and provides them with the confidence when working or studying with us.

Office 365 Backups

Following on from a procurement exercise we have implemented an Office 365 backup solution from DataVita (who provide our Datacentre solution) called Druva.

This has been setup, configured and tested over the past few weeks and is now fully operational thus mitigating the risk of data loss to the college in the event of a cyber-incident or user error which impacts on our Office 365 data (Exchange, SharePoint, OneDrive and Teams)

This adds to the comprehensive backup and disaster recovery solution we have in place with Data Vita for our servers/data putting the college in a great place to minimise data loss across all our data stores should an cyber incident occur.

Disaster Recovery Testing

As part of our datacentre provision with Data Vita we have Disaster Recovery As A Service (DRAAS). The replicates all our data on an hourly basis to a secondary datacentre located in Edinburgh in the event of a major incident within the primary datacentre which is located in Chapelhall (near Airdrie).

Although this is configured we have yet to fully test this. We plan to perform this test over the period of a week where we would flip over to the secondary datacentre on a Monday morning, use it for a week and then return to the primary datacentre on the following Monday.

We plan to do this over the Easter holidays and will work with Data Vita to arrange this and communicate to the college as when we flip over and back there will be a small period of downtime.

Cyber Security Insurance

To enhance our recovery in the event of a cyber-attack we now have Cyber Insurance in place with CFC.

The main risk of a cyber-attack would be an inability to access any data until restored by our ISLT team and the cause of the attack has been identified and removed. This would make day to day operations virtually impossible during that time. Although data loss is mitigated by the transfer of data to DataVita it does not eliminate that risk of an attack.

In additional to the time spent recovering the data, the high cost in relation to the expertise in assisting the college with the recovery and identifying the source of the attack will be covered in any policy taken out.

The policy will not only provide experts in the relevant areas but also cover the costs for such outlays as Incident Response, Legal Costs, Security and Forensic Costs, Crisis Communication, Privacy Breach Management amount others.

VPN

We are in the process of moving staff over to a new VPN solution to allow continued access to our systems when working remotely.

The licence for our current VPN (Cisco AnyConnect) solution ends in February and moving to the new solution (FortiClient) provides multiple benefits-

- One of the 'medium' recommendations from our Cyber Review in 2021 suggested we consolidate our firewalls. This solution removes additional Cisco infrastructure as the new FortiClient solution uses our existing Firewall hardware thus achieving this recommendation.
- The 2FA (2 factor authentication) method used by the new FortiClient solution when users connect is the same method which they use when accessing O365 applications rather than a separate application they currently use when using the current Cisco VPN. This enhances the end user experience.
- Cost saving in hardware maintenance and software licences for the Cisco solution as well as software licences for the 2FA method which the Cisco solution used.

IT Audit

During the month of November we worked with our auditors Wylie & Bisset to complete our IT Systems Audit which concentrated on our security and processes.

I am delighted to say that the final report was received just before Christmas coming back with a 'Strong' Overall Conclusion with a couple of low recommendations which we will implement in due course.