College Sample Pty Ltd

Cyber Security Assessment focused on secure handling of PII and Sensitive College Data and ensuring Compliance.

Audience: Board/C Suite/Senior Management

GuardWare ASSESSOR

GuardWare ASSESSOR

Briefing Intent

- This sample is indicative of the report which you'll receive at the end of an assessment.
- This redacted report is from assessments done on a number of Colleges and Organisations.
- The report provides clarity around the type of user behaviour, data movement and cyber risks that you can expect to be covered during the assessment.

Assessment Scope

The scope of GuardWare Assessment is to assess customer's current security processes and controls (ISMS) based on the following criteria:

1. **Ability to securely handle sensitive data namely PII information in line with the requirements of Australian Privacy Principals and NDB Scheme.**
2. **Ability to securely handle commercially sensitive data in line with ISO/IEC 27001, ACSC Essential 8 and ACSC Information Security Manual (ISM) recommendations.**
3. **Assess current state of IT Security Governance in line with cyber security controls and the ability to handle a data breach.**

Note: Physical security of office environment and equipment is out of scope for this project.

Executive Summary

Monitoring done from 26th Nov to 13th Dec 2022

158 users monitored on 146 devices

College faces considerable risk of a Data Breach.

Assessment showcased risky handling of PII data.

The assessment has shown that the College lacks data monitoring controls and faces the risk of losing sensitive IP either due to human error or malicious intent.

During the assessment 2 suspicious activities regarding College IP were also detected which need urgent action.

College lacks full implementation of ACSC ES8 controls. Two of the controls being detected as failing.

The College doesn't have any IT Security Governance processes in place. This further increases the risk of data loss and breach.

College is advised to take immediate actions to rectify the current state of cyber security. A list of recommendations based on their priority is provided at the end of this document.

ISMS Evaluation Criteria	Implementation level	Risk Level (High, Medium, Low)
Ability to securely handle sensitive data namely PII information in line with the requirements of Australian Privacy Principals and NDB Scheme.	**20%**	**High**
Ability to securely handle commercially sensitive data in line with ISO/IEC 27001, ACSC Essential 8 and ACSC Information Security Manual (ISM) recommendations.	**20%**	**High**
Assess current state of IT Security Governance in line with cyber security controls and the ability to handle a privacy breach.	**20%**	**High**

16 High risk actions detected which require urgent attention

4 Medium risk actions detected

2 suspicious activities detected – Need urgent action

Non-Compliance to ES8 and when handling PII data

Risk Summary

IT Governance Summary

No	IT Governance Aspect	Implemented/Partial/ Not Implemented	Risk Level No Risk, Low, Medium, High)
1	Information security policies	Not Implemented	High
2	Organisation of information security	Partial	Medium
3	Ensuring responsible use of information assets	Partial	High
4	Control Access of data (Access control)	Partial	medium
5	Ensuring data is secure when stored. (Data at rest)	Partial	Low
6	Monitoring Movement of Data (Data Egress Monitoring)	Not Implemented	High
7	Supply chain security	Not Implemented	High
7	Information security incident management	Partial	High

GuardWare

Data Handling Risk Summary

Monitoring Parameters:

- Only customer owned devices were covered.

- The following types of data were monitored:
  - Sensitive PII data covering TFN, Credit Card, Mobile numbers, Account numbers, Medicare Numbers, Name and Address.
  - Generic College IP Documents
  - General files of any type including source code, images, zip etc

- Monitoring USE CASES included those recommended under ACSC ISM around Insider Threats and Secure handling of PII Data

Monitoring done from 26th Nov to 13th Dec 2022	**158 users monitored on 146 devices**
16 High risk actions detected which require urgent attention	**4 Medium risk actions detected**
2 suspicious activities detected – Need urgent action	**No controls in place to ensure secure handling of Sensitive data**
No incident detection capability present in the event of a loss or theft of data	**Non-Compliance with 2 of ES8 control. App Control and Restrict Admin privileges**

Use Cases	Technical Control Implemented/Partial/Not Implemented/Failed Control	Risk Level (No Risk, Low, Medium, High)
PII and Sensitive College IP transferred using external storage media		
High use of unencrypted USBs. 44 users detected using unencrypted USBs to transfer data.	Technical control not implemented	High
High transfer rate. 8 users transferred over 1000 files.	Technical control not implemented	High
Outside of normal business hours. High rate of transfers detected outside of normal working hours.	Technical control not implemented	High
Transfer of Potential Sensitive Data. • Top 8 users detected transferring 1000s of design related files. • Several users transferred files containing potential sensitive data	Technical control not implemented	High
Visibility of transfers. Visibility of sensitive data transferred using external media	Technical control not implemented	High
Suspicious User Activities		
Suspicious User Activity – User1 - **Use of personal emails to send corporate data** 1. User detected using his personal email to send highly sensitive Intellectual Property marked data to unauthorized 3rd parties.	Technical control not implemented	High
Suspicious User Activity – User2 – **Data copied by user about to leave the organisation.** 1. User copied 1000s of design files also printed his CV during the same time. 2. There is evidence he has visited job sites (Indeed) and applied for related engineering jobs around the same time when he copied the files. 3. The files have been copied on unencrypted USBs which most likely are personal. 4. He is also seen accessing and uploading files to personal Google Drive. 5. He belongs to the Engineering User Group.	Technical control not implemented	High

GuardWare

Use Cases	Technical Control Implemented/Partial/Not Implemented/Failed Control	Risk Level (No Risk, Low, Medium, High)
Corporate Email Analysis – PII Data forwarded by staff to personal emails.		
Customer data forwarded to personal emails by staff. Email detected being forwarded to user own personal email.	Technical control not implemented	Medium
Visibility of email forwards. Visibility of what files have been forwarded by users to personal and free emails to ensure they are accounted for.	Technical control not implemented	High
Use of Personal Emails		
Use of Personal emails detected. Personal emails have been used to send data.	Technical control not implemented	High
Visibility of Personal Email Use. Visibility is required to ensure College data is not being sent out via personal emails.	Technical control not implemented	High
Use of Non-Organisational Unauthorised Applications		
Technical Control Circumvented. The users seem to have found a way to install non-organisational applications. **Non-Compliance of 2 of the ES8 Controls.** 1. Restrict administrative privileges 2. Application control	Failed Technical Control	High
Visibility of Application Use. Visibility of what applications are being used by users.	Technical control not implemented	High
PII data transfers using Cloud Applications and non-organizational websites		
Risky Transfer Application Use. 6 users detected using Dropbox or Google Drive to transfer files. Transfers include potentially sensitive data.	Failed Technical Control	High
Risky website Use.19 users detected using Facebook and potentially transferring data.	Technical control not implemented	High
Visibility of transfers. Visibility of sensitive data transferred using APPs and encrypted websites.	Technical control not implemented	High

Use Cases	Technical Control Implemented/Partial/Not Implemented/Failed Control	Risk Level (No Risk, Low, Medium, High)
Printing of PII Data		
Printing of potential sensitive data. Printing of sensitive data was observed.	**Technical control not implemented**	**Medium**
Printing use personal Printers. As users are allowed to work from home there is risk of files being printed using home printers.	**Technical control not implemented**	**Medium**
Visibility of Printing. Visibility of what files have been printed either via organisational or personal printers to ensure they are accounted for.	**Technical control not implemented**	**Medium**
Access of information		
Authorised Access of sensitive Information. Ensuring authorised users can access files	**Implemented**	**No Risk**
Access Visibility. Visibility of who is accessing what files	**Implemented**	**No Risk**

Trusted Insider Program monitoring suggestion as per ACSC ISM

Trusted insider program

As a trusted insider's system access and knowledge of business processes often makes them harder to detect, establishing and maintaining a trusted insider program can assist an organisation to detect and respond to trusted insider threats before they occur, or limit damage if they do occur. In doing so, an organisation will likely obtain the most benefit by logging and analysing the following user activities:

1. excessive copying or modification of files
2. unauthorised or excessive use of removable media
3. connecting devices capable of data storage to systems
4. unusual system usage outside of normal business hours
5. excessive data access or printing compared to their peers
6. data transfers to unauthorised cloud services or webmail
7. use of unauthorised Virtual Private Networks, file transfer applications or anonymity networks.

Control: ISM-1625; Revision: 1; Updated: Dec-22; Applicability: All; Essential Eight: N/A
A trusted insider program is developed, implemented and maintained.

Control: ISM-1626; Revision: 0; Updated: Nov-20; Applicability: All; Essential Eight: N/A
Legal advice is sought regarding the development and implementation of a trusted insider program.

Reference: ACSC Information Security Manual.

Mapping to Trusted Insider USE CASEs as per ACSC ISM

Recommended Use Cases Under ISM	Detected/Not Detected/Not Tested
excessive copying or modification of files	Detected
unauthorised or excessive use of removable media	Detected
connecting devices capable of data storage to systems	Detected
unusual system usage outside of normal business hours	Detected
excessive data access or printing compared to their peers	Detected
data transfers to unauthorised cloud services or webmail	Detected
use of unauthorised Virtual Private Networks, file transfer applications or anonymity networks.	Detected

SharePoint Risks

Covers Sharing and access of files by internal and external users.

SharePoint Risk – Monitoring and Control of External User Access

SharePoint Risk		
Visibility of Downloads of Files by internal and external users. Visibility of what files have been downloaded by internal and external users. Once downloaded, we lose control over the data.	**Technical control not implemented**	**High**
Visibility of Shared Files to external users. Visibility of what files have been shared to external users.	**Technical control not implemented**	**High**

SharePoint is Defacto File server for most organisations which is accessible from anywhere and from any device including personal devices.

Risk 1: Monitoring of files accessed by internal and external users is critical to ensure security of data.

Risk 2: Wrong configuration of libraries can easily result in access of sensitive data by internal and external users when shared.

Risk 3: Sensitive data can be shared accidentally to unauthorised external users.

Sharepoint Access External

Search | Per Page 50

By File | By User

File Name	Number of Users	Number of Incidents
e-Safe Compliance User Manual v2 Draft 4.docx	1	18
Excercise 1 Map the data to its classification .docx	1	8
Guardware - Data Monitoring and scoping form v3.xlsx	1	11
Guardware Company Decisions.xlsx	1	8
GuardWare INSIGHT User Manual v2.pdf	1	6

Sharepoint Access External > GuardWare INSIGHT User Manual v2.pdf

Search

By User

User Name	Email Address	Site Url	File Path	Date Time	Incident Type
richard	richard@gmail.com	https://guardwarecomau.sharepoint.com/sites/GuardWareSupport	Shared Documents/Trainings and help files/Overall System Manual/	2025-01-24 04:34:32	AnonymousLinkUsed
richard	richard@gmail.com	https://guardwarecomau.sharepoint.com/sites/GuardWareSupport	Shared Documents/Trainings and help files/Overall System Manual/	2025-01-24 04:34:32	SharingLinkUsed
selina	selina@yahoo.com	https://guardwarecomau.sharepoint.com/sites/GuardWareSupport	Shared Documents/Trainings and help files/Overall System Manual/	2025-01-10 04:15:35	AnonymousLinkUsed
selina	selina@yahoo.com	https://guardwarecomau.sharepoint.com/sites/GuardWareSupport	Shared Documents/Trainings and help files/Overall System Manual/	2025-01-10 04:15:35	SharingLinkUsed

SharePoint Risk – Files downloaded to personal devices. There is a need for Visibility.

Sharepoint Audit Logs

Search

By File By Platform By IP address

Platform Name	Secure link created	Anonymous Link Created	Accessed by(internal)	Accessed by(external)	Downloaded by(internal)	Downloaded by(external)
-	0	0	8,735	37	0	0
Android	1	0	6	0	1	0
iPhone	0	0	32	5	11	0
MacOSX	1	15	47	35	10	6
NotSpecified	82	0	622	16	115	0
OfficeCollaborationService	0	0	50	0	0	0

- **Files downloaded by users which can be to Corporate and personal devices**
- **Need to ensure visibility of data.**

Android	
Accessed by(internal)	Downloaded by(internal)
Username	Username2
rizwan.m	simon.s
grishma.k	
roshan.b	

MacOSX		
Anonymous Link Created	Accessed by(external)	Downloaded by(external)
Username3	Username4	Username5
pritijan.m	anonymous	anonymous
rabin.t		
prakash.c		

IPhone		
Accessed by(internal)	Accessed by(external)	Downloaded by(internal)
Username6	Username7	Username8
richard.m		akhil.s
akhil.s		richard.m
		selina.t

Risky Sharing of Data

Data transfer using external storage media		
Files shared using anonymous links to external users..	Technical control not implemented	High
Sensitive files shared to external users. Potential Unauthorised access.	Technical control not implemented	High

Sharepoint has made access and sharing of information incredibly easy and accessible from anywhere. Unfortunately, users often tend to have the false sense of security that all data in SharePoint is secured. Reality is if SharePoint is not configured properly and monitored it can easily become a major source of data leak.

Risk 1: Anonymous sharing is a risky action. As external users can simply share and access the link without any check and balance.

Risk 2: Sensitive data can be maliciously or unknowingly shared by authorised users to internal or external unauthorized users**.**

Anonymous Sharing of files

File Name	Anonymous Link Created	Accessed by(internal)	Accessed by(external)
GuardWare INSIGHT User Manual v2.pdf	1	15	6

Sensitive data accessed by external users

SharePoint Risk → Ensure Authorised Internal Company Access to libraries and files.

Sharepoint Library

Search

Library Name

User Name	Library Name	Site Name	File Name	Secure link created	Anonymous Link Created	Accessed by(internal)	Accessed by(external)	Downloaded by(internal)
selina.t	Shared Documents/Development/DevelopmentPlan/	https://guardwarecomau.sharepoint.com/Documents/INSIGHTDevelopment/	GuardWare INSIGHT User Manual v2.pdf	0	1	15	6	0
akhil.s	Deployment/Report/	https://guardwarecomau.sharepoint.com/Documents/Schedule/	INSIGHT Report Update v1.docx	0	0	26	5	15

Sharepoint Library > Accessed By (Internal) > Shared Documents/Development/DevelopmentPlan/

Search | Per Page 10

By User

User Name	Email Address	SiteUrl	File Path	Incident Date	Incident Time	Incident Type
selina.t	selina.t@guardware.com.au	https://guardwarecomau.sharepoint.com/Documents/INSIGHTDevelopment/	Shared Documents/Development/DevelopmentPlan/	2024-12-30	07:14:10	FilePreviewed
selina.t	selina.t@guardware.com.au	https://guardwarecomau.sharepoint.com/Documents/INSIGHTDevelopment/	Shared Documents/Development/DevelopmentPlan	2024-12-30	22:39:51	FilePreviewed

- **Access and download of files by users. Need to ensure it is authorised access.**
- **Need to ensure visibility of data.**

Anonymous Access - SharePoint Risk

Sharepoint File log > Anonymous Link Created > File name > GuardWare INSIGHT User Manual v2.pdf

Search

By User

User Name	Site Url	File Path	Email Address	Incident Date	Incident Time	Incident Type
akhil.s	https://guardwarecomau.sharepoint.com/sites/GuardWareSupport	Shared Documents/Trainings and help files/Overall System Manual/	akhil.s@guardware.com.au	2025-01-09	07:49:24	AnonymousLinkCreated

Sharepoint File log > Downloaded By (External) > File name > GuardWare INSIGHT User Manual v2.pdf

Search

By User

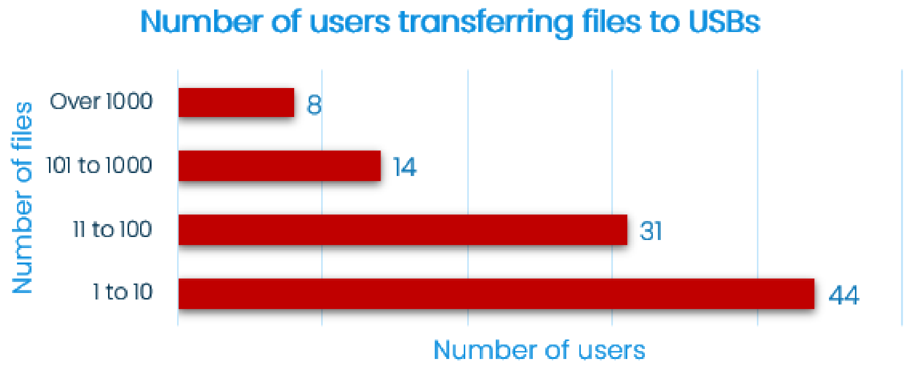
User Name	Site Url	File Path	Email Address	Incident Date	Incident Time	Incident Type
anonymous	https://guardwarecomau.sharepoint.com/sites/GuardWareSupport/	Shared Documents/Trainings and help files/Overall System Manual/	anonymous	2025-01-24	04:34:38	FileDownloaded
anonymous	https://guardwarecomau.sharepoint.com/sites/GuardWareSupport/	Shared Documents/Trainings and help files/Overall System Manual/	anonymous	2025-01-10	04:15:41	FileDownloaded
anonymous	https://guardwarecomau.sharepoint.com/sites/GuardWareSupport/	Shared Documents/Trainings and help files/Overall System Manual/	anonymous	2025-01-10	05:58:53	FileDownloaded

Storage Media Analysis

Covers all types of media including phone sync.

PII and Sensitive College Data transfer using external storage media

Data transfer using external storage media		
High use of unencrypted USBs. 44 users detected using unencrypted USBs to transfer data.	Technical control not implemented	High
High transfer rate. 8 users transferred over 1000 files.	Technical control not implemented	High
Outside of normal business hours. High rate of transfers detected outside of normal working hours.	Technical control not implemented	High



User Name	User Group	Total Events
xxxxx	Customer Group	26256
xxxxx	Customer Group	5221
xxxxx	Customer Group	4212
xxxxx	Customer Group	3362
xxxxx	Customer Group	2326
xxxxx	Customer Group	2125
xxxxx	Customer Group	1782
xxxxx	Customer Group	1506
xxxxx	Customer Group	9
xxxxx	Customer Group	5
xxxxx	Customer Group	4
xxxxx	Customer Group	3
xxxxx	Customer Group	2
xxxxx	Customer Group	2

Hour	Working Day	Non-Working Day
0:00 - 1:00	0	0
1:00 - 2:00	0	0
2:00 - 3:00	0	0
3:00 - 4:00	0	0
4:00 - 5:00	0	0
5:00 - 6:00	0	0
6:00 - 7:00	0	0
7:00 - 8:00	0	0
8:00 - 9:00	562	0
9:00 - 10:00	41	320
10:00 - 11:00	10	8798
11:00 - 12:00	2	331
12:00 - 13:00	2221	4444
13:00 - 14:00	14	2144
14:00 - 15:00	5312	0
15:00 - 16:00	18620	0
16:00 - 17:00	421	0
17:00 - 18:00	2904	0
18:00 - 19:00	7563	0
19:00 - 20:00	33111	0
20:00 - 21:00	7	0
21:00 - 22:00	5	0
22:00 - 23:00	2	0
23:00 - 24:00	2	0

The use of USBs may be for legitimate reasons but there are significant risks involved.

Risk. Loss of phone or USBs is a common source of data breach and should be monitored and accounted for.

Risk. Potential Insider risk. Non-compliant with Trusted Insider Program monitoring requirements as per the ISM.

Risk. Compromise of sensitive corporate information. There should be a valid NEED for transferring sensitive corporate information and there should be appropriate visibility to ensure Insider Threat Management and Incident Response in case of loss.

Risk. Use of unencrypted USBs can easily lead to Data loss

Movement of Sensitive PII and IP Data using USBs

Data transfer using external storage media		
Transfer of Potential Sensitive Data. • Top 8 users detected transferring 1000s of design related files. • Several users transferred files containing potential sensitive data	**Technical control not implemented**	**High**
Visibility of transfers. Visibility of sensitive data transferred using external media	**Technical control not implemented**	**High**

Risk. Without the ability to monitor what is transferred, the College will not even know if data is lost or stolen and will not be able to perform Incident management.

Risk. Potential Insider risk. Non-compliant with Trusted Insider Program monitoring requirements as per the ISM.

Risk. Compromise of sensitive corporate information. There should be a valid NEED for transferring sensitive corporate information and there should be appropriate visibility to ensure Insider Threat Management and Incident Response in case of loss.

Risk. Use of unencrypted USBs can easily lead to Data loss

User 1

08-12-2022	7:38:45	07[redacted]c9.svn-base
08-12-2022	7:38:51	02[redacted].svn-base
08-12-2022	7:38:54	067[redacted]89.svn-base
08-12-2022	7:38:54	06[redacted]c.svn-base
08-12-2022	7:38:54	[redacted].drl
08-12-2022	7:38:54	[redacted].cmp
08-12-2022	7:38:54	[redacted].sol
08-12-2022	7:38:54	[redacted].drd
08-12-2022	7:38:54	[redacted].cmp
08-12-2022	7:38:54	[redacted].stc
08-12-2022	7:38:54	[redacted]oles.txt
08-12-2022	7:38:54	[redacted]s.txt
08-12-2022	7:39:11	[redacted]oles.txt
08-12-2022	7:39:11	[redacted]es.txt

User 2

29-11-2022	8:21:51	[redacted]_cad.csv
29-11-2022	12:30:21	[redacted]nse2.pdf
29-11-2022	12:30:21	[redacted].pdf
29-11-2022	12:30:21	[redacted]_bom.csv
29-11-2022	12:30:21	[redacted]_cad.csv
29-11-2022	12:30:21	[redacted]_bom.csv
29-11-2022	12:30:21	[redacted]_cad.csv
05-12-2022	10:23:43	[redacted].csv
05-12-2022	10:23:43	[redacted]csv

User 3

09-12-2022	7:48:12	[redacted]_power.csv
09-12-2022	7:48:12	[redacted]_spectrum.csv
09-12-2022	7:48:12	[redacted].png
09-12-2022	7:48:12	[redacted]png
09-12-2022	7:48:12	[redacted]_1.png
09-12-2022	7:48:13	[redacted].pdf
09-12-2022	7:48:13	[redacted].csv
09-12-2022	7:48:13	[redacted].pdf

Suspicious User Activity

Suspicious User Activity – User1 - **Use of personal emails to send corporate data**

Suspicious User Activity		
Potential Insider Risk. 1. User detected using his personal email to send highly sensitive college data to unauthorized 3rd parties.	**Technical control not implemented**	**High**

Use of personal emails is a common occurrence in organisations but needs to be monitored as can lead data leak.

Risk: Use of personal emails to exfiltrate data out is consistently reported as one of the keyways data is lost or stolen in organisations and needs to be monitored.

Email violation detail	
Review Status :	Not Reviewed
Violation Date & Time :	[redacted]10:26:10
Subject :	this is the file
User Name :	[redacted]
Email Domain Used :	www.mail.google.com
From :	[redacted]@gmail.com
Recipients :	TO:[redacted]com CC: BCC:
PC Name :	[redacted]
PC Serial Number :	[redacted]
Action :	Default
View complete email	

Rules Violated
[redacted]
Document Movements
General File Movement

Email Body/File Attachment
New Design Specs - Copy.docx

Detected content in email body / file attachment

Word	Context
CONFIDENTIAL	[redacted] private management confidential [redacted]
MANAGEMENT	[redacted] systems private management confidential [redacted]

Suspicious User Activity – User2 – Data copied by user about to leave the organisation.

GuardWare

Suspicious User Activity		
Potential Insider Risk. 1. User copied 1000s of design files, also printed his CV during the same time. 2. There is evidence he has visited job sites (Indeed) and applied for industry related engineering jobs around the same time when he copied the files. 3. The files have been copied on unencrypted USBs which most likely are personal. 4. He is also seen accessing and uploading files to personal Google Drive. 5. He belongs to the Engineering User Group.	**Technical control not implemented**	**High**

Risk. Rapid and frequent transfer of large amounts of College data, the fact that the user is reviewing his CV and is applying for jobs are all tell-tale signs of a potential insider threat in progress.

Risk. The user has personal Dropbox installed meaning he has circumvented College policy.

Print Event List for XXXXX using printer Canon-X53Series

User Name	User Group Name	PC Name	File Name	Event Date	Event Time	File Path
XXXXX	[redacted]	LAP2u82	my cv 2022.docx	02-12-2022	13:40:55	c:\users\XXXX\Downloads\my cv 2022.doc

Data copied to 2 distinct unencrypted USBs. Early Morning and on Weekend.

Serial Number	Insertion Date/Time	Removeal Date/Time	Number Files
531455422	2022-12-18 22:20:16	2022-12-18 00:00:00	9685
531455422	2022-12-18 09:47:04	2022-12-18 10:20:16	6622
931222212	2022-12-25 08:31:19	2022-12-25 09:47:04	15633
931222212	2022-12-25 19:35:33	2022-12-25 20:31:19	8952

GuardWare

Suspicious User Activity- User 1

Applying for Jobs on Indeed.com the next day.

Date/Time	Duration	Full URL
2022/12/03 17:00:00	0:05:36	au.indeed.com/[redacted]edabda9de58bfe0f2ff
2022/12/03 17:30:00	0:18:41	au.indeed.com/[redacted]
2022/12/03 17:00:00	0:01:40	au.indeed.com/job/[redacted]c
2022/12/03 17:00:00	0:01:30	au.indeed.com/job/[redacted]
2022/12/03 17:00:00	0:01:09	au.indeed.com/job/[redacted]f
2022/12/03 17:00:00	0:01:10	au.indeed.com/job/[redacted]f
2022/12/03 17:00:00	0:00:50	au.indeed.com/job/[redacted]f
2022/12/03 17:00:00	0:00:44	au.indeed.com/companies/[redacted]
2022/12/03 17:00:00	0:00:41	au.indeed.com/companies/[redacted]
2022/12/03 17:00:00	0:00:36	au.indeed.com/companies/[redacted]
2022/12/03 17:00:00	0:00:29	au.indeed.com/job/[redacted]0
2022/12/03 17:00:00	0:00:26	au.indeed.com/job/[redacted]f6
2022/12/03 17:00:00	0:00:25	au.indeed.com/job/[redacted]
2022/12/03 17:00:00	0:00:23	au.indeed.com/job/[redacted]
2022/12/03 17:30:00	0:00:23	au.indeed.com/job/[redacted]
2022/12/03 17:00:00	0:00:16	au.indeed.com/job/[redacted]
2022/12/03 17:00:00	0:00:13	au.indeed.com/job/[redacted]77
2022/12/03 17:00:00	0:00:11	au.indeed.com/job/[redacted]b5
2022/12/03 17:00:00	0:00:11	au.indeed.com/job/[redacted]
2022/12/03 17:30:00	0:00:11	au.indeed.com/job/[redacted]
2022/12/03 17:00:00	0:00:06	au.indeed.com/job/[redacted]f
2022/12/09 17:30:00	0:00:06	au.indeed.com/job/[redacted]
2022/12/03 17:00:00	0:00:04	au.indeed.com/job/[redacted]
2022/12/03 17:30:00	0:00:04	au.indeed.com/job/[redacted]6
2022/12/03 17:00:00	0:00:03	au.indeed.com/job/[redacted]

Email Analysis

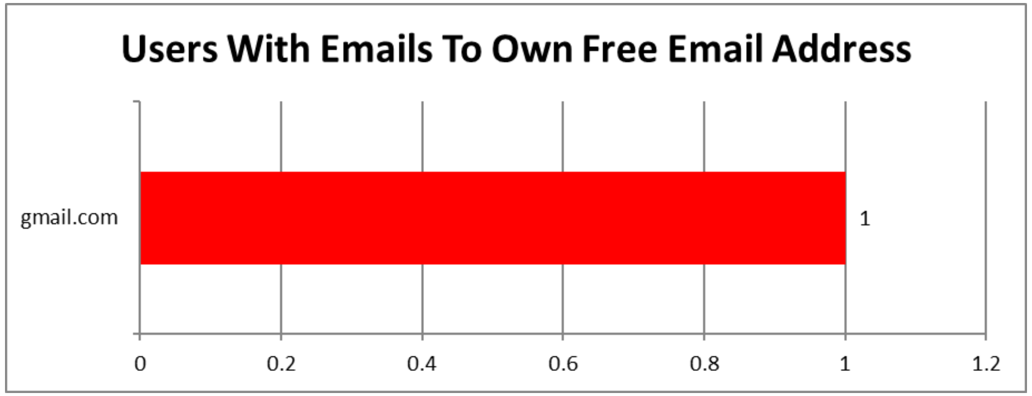
Covers both Corporate and Personal Email transactions.

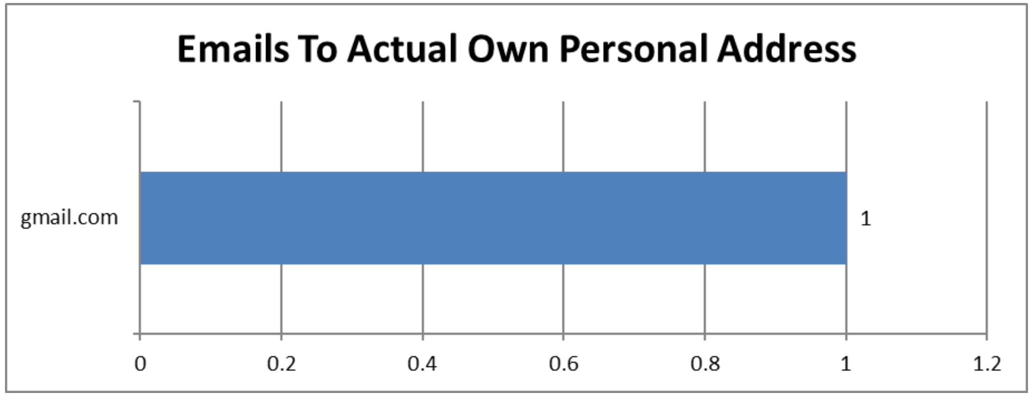
Customer data forwarded to personal emails

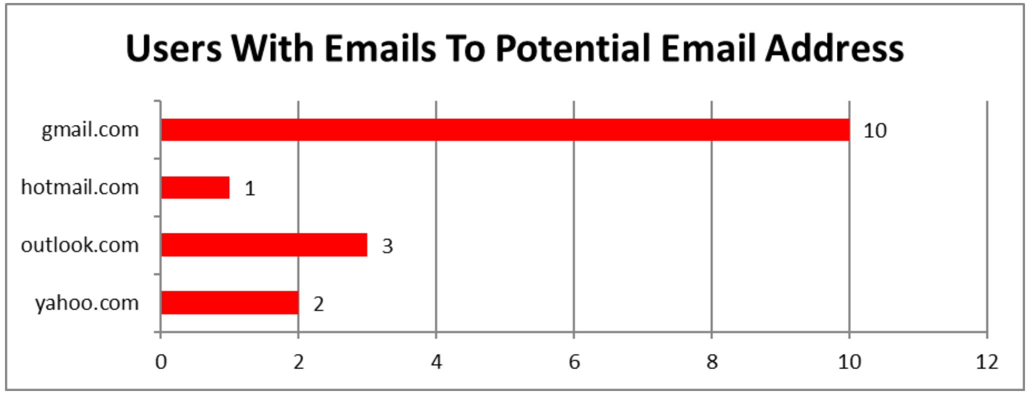
Corporate Email Analysis		
Customer data forwarded to personal emails by staff. Email detected being forwarded to user own personal email.	Technical control not implemented	Medium
Visibility of email forwards. Visibility of what files have been forwarded by users to personal and free emails to ensure they are accounted for.	Technical control not implemented	High

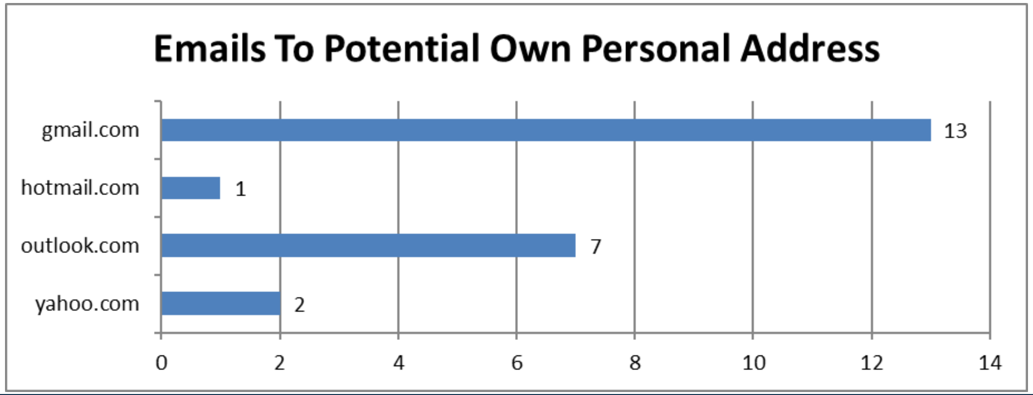
Forwarding emails to personal and other free emails is a common cause of leakage and non-compliance

Risk: Forwarding corporate information to personal emails leads to information creep. The action needs to be checked in the event sensitive information is forwarded to free emails.



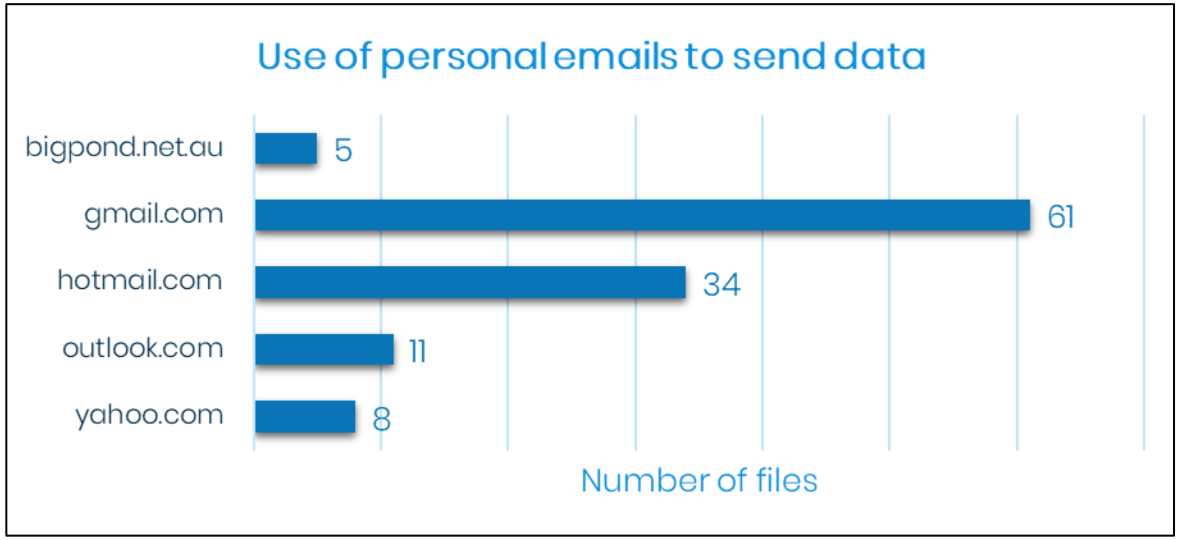






Use of personal emails to send data

Use of Personal Emails		
Use of Personal emails to send corporate data detected. Personal emails have been used to send corporate data.	Technical control not implemented	High
Visibility of Personal Email Use. Visibility is required to ensure College data is not being sent out via personal emails.	Technical control not implemented	High



Use of personal emails is a common occurrence in organisations but needs to be monitored as can lead to data leaks.

Risk: Use of personal emails to exfiltrate data out is consistently reported as one of the key ways data is lost or stolen in organisations and needs to be monitored.

Use of Non-Organisational Unauthorised Applications

Non-Compliance of 2 of the ES8 Controls.

1. Restrict administrative privileges
2. Application control

Installation and Use of Non-organisational applications

Data transfer using non-corporate applications		
Technical Control Circumvented. The users seem to have found a way to install non-organisational applications. **Non-Compliance of 2 of the ES8 Controls.** 1. Restrict administrative privileges 2. Application control	**Failed Technical Control**	**High**
Visibility of Application Use. Visibility of what applications are being used by users.	**Technical control not implemented**	**High**

Software Name	Vendor	Number of PCs with Software Present	Number of PCs with Software Usage	Total Usage Duration
MESSENGER.EXE	Facebook Inc.	5	3	1:15:00
TELEGRAM.EXE	Telegram	5	2	0:41:40
WHATSAPP.EXE	WhatsApp	6	2	0:17:30
FILEZILLA.EXE	FileZilla Project	1	1	0:08:41
DROPBOX.EXE	Dropbox, Inc.	8		
OPERA.EXE	Opera Software	2		

The use of personal applications without proper authorization and vetting may be for legitimate reasons, but there are significant risks involved.

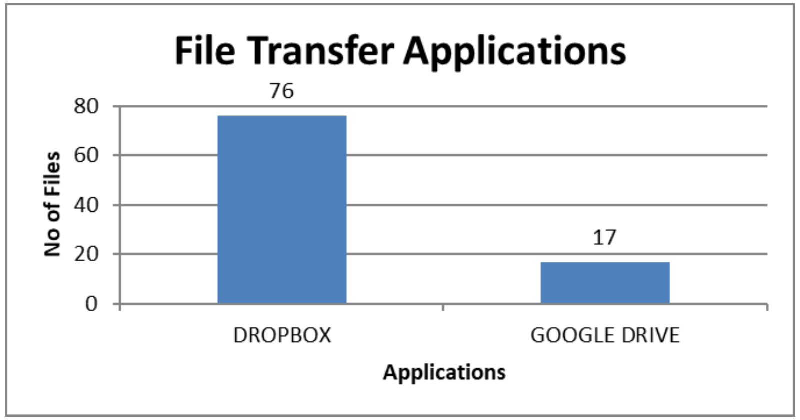
Risk. Standard users should not have admin rights to install applications. It can result in malware infection and highlights that the current controls are failing to implement 2 of the ES8 Controls.

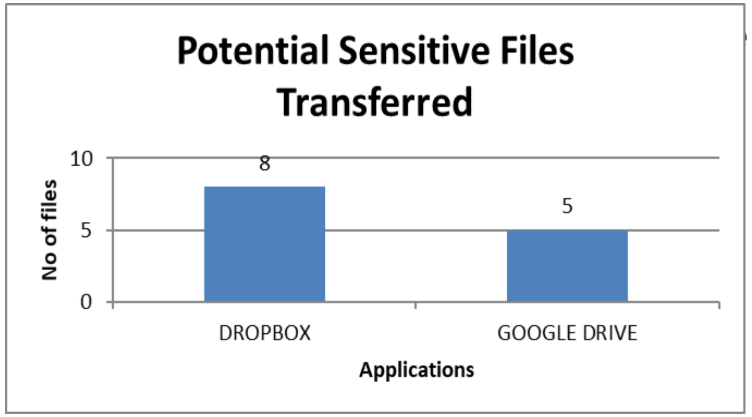
1. Restrict administrative privileges
2. Application control.

Data transfer using Non-Corporate Data sharing Apps and Websites

PII data transfers using Cloud Applications

Data transfer using non-corporate applications		
Risky Transfer Application Use. 6 users detected using Dropbox or Google Drive to transfer files. Transfers include potential sensitive data.	**Failed Technical Control**	**High**
Visibility of transfers. Visibility of sensitive data transferred using external media	**Technical control not implemented**	**High**





User Name	User Group	Total Events
xxxxxx	Client Group	34443
xxxxxx	Client Group	1722
xxxxxx	Client Group	1428
xxxxxx	Client Group	17

The use of personal cloud services and applications may be for legitimate reasons, but there are significant risks involved.

Risk. Unauthorized access by former staff members. Information stored in personal cloud account remains with its user after he leaves a College and therefore can result in a breach as per NDB Scheme.

Risk. Applications like Dropbox, OneDrive, and Google Drive sync files to any device where a user is logged into these applications. This may include their personal devices or, even worse, those of a different College, which could result in the loss of sensitive information.

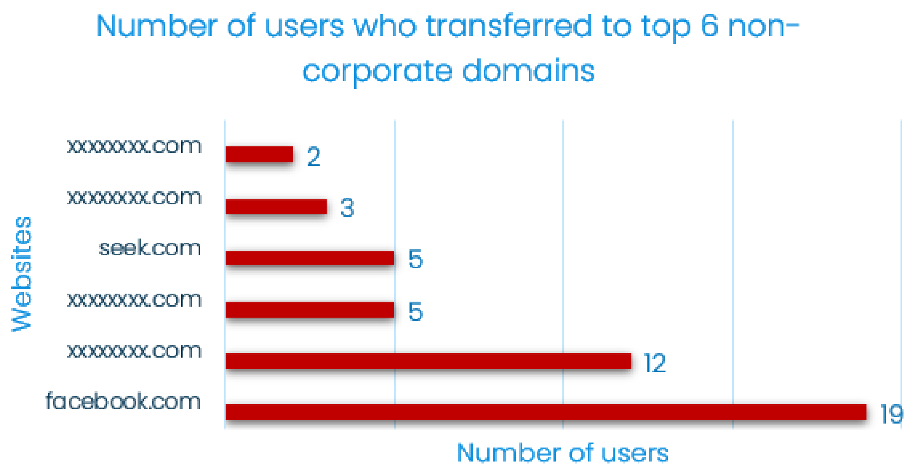
29-11-2022	14:03:28	DROPBOX	1231212.docx
29-11-2022	14:03:28	DROPBOX	1-product comparison-latest- jun 2018 copy.xlsx
29-11-2022	14:03:28	DROPBOX	1-product comparison-latest- jun 2018.xlsx
29-11-2022	14:03:29	DROPBOX	1231212_00.docx
29-11-2022	14:03:29	DROPBOX	1231212_00_11.docx
29-11-2022	14:03:29	DROPBOX	amex2222_3.xls
29-11-2022	14:03:29	DROPBOX	az-100.docx
29-11-2022	14:03:30	DROPBOX	capture.png
29-11-2022	14:03:30	DROPBOX	claim - copy.xls
29-11-2022	14:03:43	DROPBOX	client4.4.0.10 - lc-temora.msi
29-11-2022	14:03:56	DROPBOX	contract form.doc
29-11-2022	14:03:56	DROPBOX	creditcard.docx
29-11-2022	14:03:57	DROPBOX	customer info.xlsx
29-11-2022	14:03:57	DROPBOX	customer_info.docx
29-11-2022	14:03:58	DROPBOX	customer_offer letter.docx

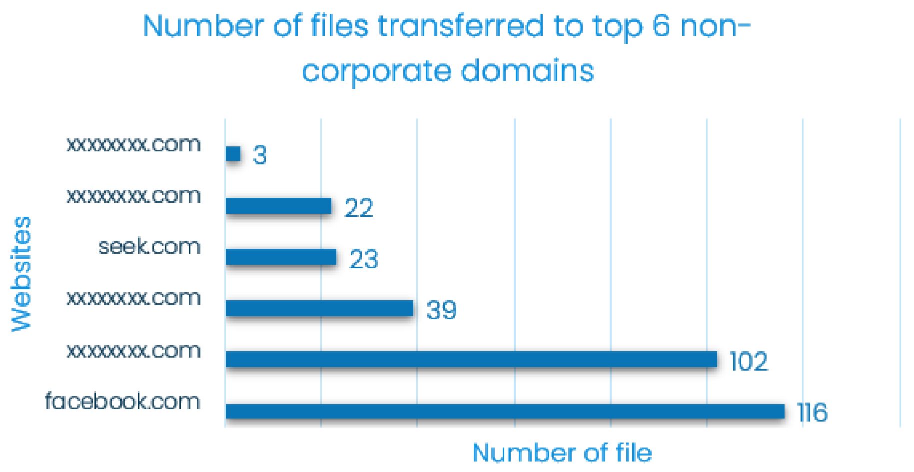
Data transfer using Non-organisational websites

Data transfer using non-corporate applications		
Risky website Use. 19 users detected using Facebook and potentially transferring data.	Technical control not implemented	High
Visibility of transfers. Visibility of sensitive data transferred using APPs and encrypted websites.	Technical control not implemented	High

Transferring of files to non-corporate websites may be for legitimate reasons, but there are significant risks involved.

Risk. Can result in a breach if sensitive or PII data is uploaded to non-corporate websites either accidentally or due to malicious intent.





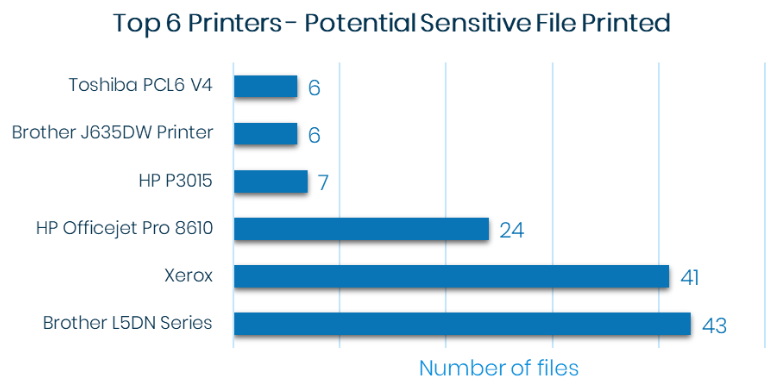
Printing Analysis

Printing of PII Information

Printing of Sensitive Data		
Printing of potential sensitive data. Printing of sensitive data was observed.	**Technical control not implemented**	**Medium**
Printing use personal Printers. As users are allowed to work from home there is risk of files being printed using home printers.	**Technical control not implemented**	**Medium**
Visibility of Printing. Visibility of what files have been printed either via organisational or personal printers to ensure they are accounted for.	**Technical control not implemented**	**Medium**

The use of these printers may be for legitimate reasons but can result in a breach.

Risk. According to ACSC Loss of printed information is a common occurrence leading to a data breach. As such printing of material needs to be monitored and controlled. Users should be made responsible for the security of printed materials. All printing events need to be monitored.



Printer Name	Total Events
\\rbcmon02\[redacted]-Office	25
\\RBCPRN01\[redacted]-Office	22
\\rbcprn01\[redacted]Office	19
\\RBCPRN01\[redacted]-Office	12
D-Accounts	6
Microsoft Print to PDF	5
\\rbcmon02\[redacted]-Office2	5
\\rbcprn01\[redacted]-Office	5
Microsoft Print to PDF	4
\\rbcprn01\[redacted]-Manager Office	3
Canon TS3300 series	3
OneNote for Windows 10	2
Adobe PDF	2
\\RBCPRN01\[redacted]-Office	2
I Block Lv2 Toshiba	2
[redacted]-Admin	2
HP8A771D (HP Officejet Pro 6830)	2
\\rbcprn01\[redacted]-Office	1
Adobe PDF	1
HPBBF063 (HP OfficeJet Pro 8710)	1
\\RBCPRN01\[redacted]-Office	1
[redacted]	1
HP000756 (HP Officejet 6600)	1
Brother HL-1110 series	1
Adobe PDF	1
Brother MFC-L3750CDW series Printer	1
\\RBCPRN01\[redacted]-Office	1
\\rbcprn01\[redacted]-Office	1
Canon MG6200 series Printer XPS	1

Access of files

Access of files

Access of information		
Authorised Access of sensitive Information. Ensuring authorised users can access files	**Implemented**	**No Risk**
Access Visibility. Visibility of who is accessing what files	**Implemented**	**No Risk**

The College has visibility and means to validate if authorised users are accessing sensitive data.

DLP File Access Incidents by Rule Name

Rule Name	mber of	Number of Files
[redacted]	79	1086
Document Access	146	19567

File Name	User Name	Date	Time	File Path
mp-23 project brief.doc	[redacted]	29/11/2022	12:42:56	c:\users\User\document\Client Profile\mp-23 project brief.doc
ac_id_74 - signed.docx		29/11/2022	15:21:49	c:\users\User\document\Client Profile\ac_id_74 - signed.docx
security snippets nov 2022.pdf		29/11/2022	9:36:52	c:\users\User\document\Client Profile\\security snippets nov 2022.pdf
agreementreconciliation.pdf		29/11/2022	11:55:43	c:\users\User\document\Client Profile\agreementreconciliation.pdf
202208_client.xlsx		29/11/2022	10:13:53	c:\users\User\document\Client Profile\202208_client.xlsx
performance report.pdf		29/11/2022	11:21:31	c:\users\User\downloads\performance report.pdf
performance report (1).pdf		29/11/2022	11:21:39	c:\users\User\downloads\performance report (1).pdf
protect 1st work package costing.xlsx		6/12/2022	13:29:50	c:\users\admin\desktop\demos\project f20\protect 1st work package costing.xlsx

Recommendation to Reduce Risk

High Priority

The College's users are exhibiting several risky behaviours when dealing with College data. These are putting College IP at serious risk and can easily result in a Breach. There is a need to monitor and control these activities.

Implement a User activity Monitoring, Data Egress/leak Monitoring solution which can monitor and alert "sensitive data" in the following use cases:

- Access of sensitive files
- Transfer using corporate channels like emails and cloud.
- Transfer using any personal online sources like free emails, cloud, and web uploads.
- Transfers using encrypted personal chats like WhatsApp.
- Data shared out directly from cloud shares.
- Printed using corporate and personal printers.
- Transfer using offline sources like USBs, phone sync etc.
- Locate laptops containing Sensitive PII data
- Monitor and control syncing of data using wireless methods like Bluetooth and Mobile Sync apps.
- Ability to monitor when user's circumvent College policy.
- Monitor use of unauthorized College applications.
- Monitor access of risky websites.
- Ability to monitor 24/7 even not connected to corporate network or offline.

Recommendation to Reduce Risk

High Priority

- Implement a staff awareness program around the identified risks. The OAIC's **Guide to Securing Personal Information** sets out expectations that Entities should ensure they foster a privacy and security aware culture, such as through staff training and awareness exercises.

High Priority

- The College is recommended to complete their IT Security Policy. It is recommended that the IT Security policy covers the following areas:

  - Privacy Policy
  - Acceptable Use Policy
  - Authentical Policy
    - Password Policy
    - MFA Policy
  - Access control and Authorisation Policy
  - Data Protection Policy
    - Data classification
    - Asset register
    - Protection of assets
  - Communication and Data Transfer Policy
    - Email Policy
    - Chat
    - Media transfer
    - Other communication mechanisms.
  - Mobile Device Protection and Management Policy
    - Mobile device management
    - Mobile device encryption
  - Configuration and Vulnerability Management
    - Patching (which will include OS, and applications)
    - Application Control
    - User application hardening
    - MACRO management
    - AV configuration
  - IT equipment Purchase, Deployment and Disposal Policy
  - Clean Desk Policy
  - Business Continuity Policy
    - Business Continuity Plan.
    - Backup and recovery strategy
  - Supplier Management Policy
  - User education and awareness policy
  - Data Breach Response Plan

Recommendation to Reduce Risk

High Priority

- College should aim to meet a minimum maturity of level 1 for ACSC essential 8 controls. The following essential 8 controls are considered of higher importance:
    - Application control
    - Patch applications
    - Patch Operating System
    - Restrict administrative privileges

Medium Priority

- The following essential 8 controls are considered of medium importance:
    - Backup
    - Configure Microsoft Office macro settings
    - User application hardening

GuardWare offers products designed to keep your data safe and can help implement the recommendations in this report.

Contact Information

Level 13, 465 Victoria Avenue,
Chatswood, Sydney 2067, Australia.

Email: sales@guardware.com

Phone: +61 2 9994 8061