IT FEELS LIKE HOME FIRST IT TRAINING GUIDE

PART A (Introduction)

This document is used to train and educate IT prosomal to prevent cyberattacks and data breaches.

Part B (Summary of OS & Cyber Security Concepts)

i) Summary of OS (Operating System)

It acts as a platform between the user and the computer hardware and controls the execution of all kinds of programs.

Examples of OS: Linux Operating System, Windows Operating System, MACOS, etc.

ii) Summary of Cyber Security Concepts

Cyber Security is a big topic, but it mainly revolves around a Key Concept called "The C.I.A. Triad".

"C" stands for Confidentiality; it defines the rules that limit information access. Measures are a method to restrict sensitive information from being accessed by Cyber Attackers and Hackers.
So some of us have access to details others may not have; these permission are given to different statuses you have in the system.
There are various ways to ensure confidentiality, like two-factor authentication, Data encryption, data classification, biometric verification, and security tokens.

"I" stands for Integrity; it ensures that data is consistent, accurate and trustworthy over time.
There are many tools for us to check if there were any changes or possible data breaches.
To ensure no data loss, regular backup happens. Currently, the most trusted solution is cloud backup.

"A" stands for Availability. All necessary components like hardware, software, networks, devices, and security equipment should be maintained and upgraded to ensure smooth data functioning and access without any disruption. They are also providing constant communication between the components by providing enough bandwidth.

Part C (Computer Misuse & Cyber Security Act and Data Protection Act)

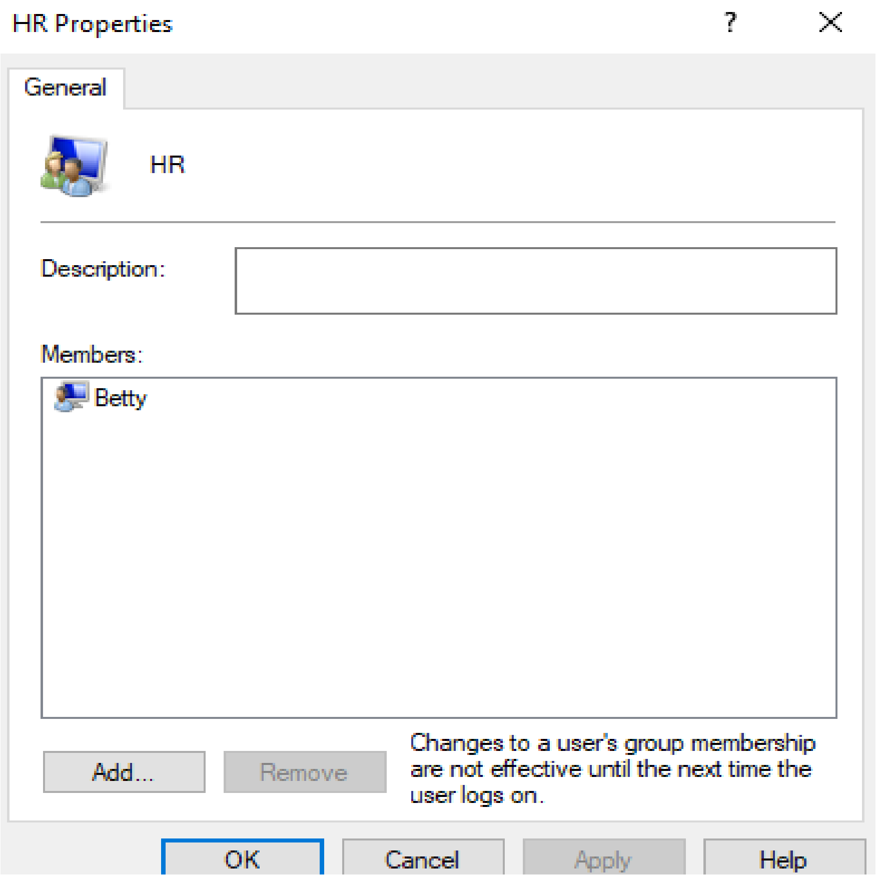
S/N	Clause	Clause Details	Impact	Recommendations	Justification for the Recommendations
1	Computer Misuse Act Part II	S3 – Unauthorized access to computer material	Unauthorised users can access and download private and confidential data.	Lock the data with password encryption and a One Time Pin with a 2nd verification system.	Limits the easy access as only staff allowed to use it are first kept in a list with their password-protected then given a particular app to verify the data.
2	Computer Misuse Act Part II	S4 – Access with the intent to commit and facilitate commissions of offence	Any person with the plan to use the computer to retrieve information and use it with a malicious intent	Limit the access of the specific network for the user. E.g: Administrator Network, Staff Network and Guest Network	Limit access to information and user controls as the different networks have different purposes.
3	Computer Misuse Act Part II	S5- Unauthorised modifications of computer material	Any unauthorised person who alter documents that they are not allowed to change.	Limit the access to authorised personnel firstly. Secondly, every time a copy is open, it will be logged by the system on who opened it and alterations changed.	This helps to trace back to the user easily as it's within a list.
4	Computer Misuse Act Part II	S6- Unauthorised use or interception of computer services	Any personal retrieving info through the unauthorised method.	Keep things in folder with limited access to the network through devices.	This means public personnel or staff has the lesser possibility to access data.
5	Computer Misuse Act Part II	S8- Unauthorised Disclose of access code	Any person knowingly and without authority disclose any password access code with the intent to gain access to any program or data	Don't leave a notepad with passwords lying around and setup verifications for staff for logging in and amending essential documents.	No matter what change you make to an important document, the user's true identity must verify it.

			for an unlawful purpose.		
6	**Personal Data Protection Act Part V**	**21-Access to personal data (3)**	**Any organisation is not required to provide an individual with the individual's data with a suspicion to threaten, cause harm or reveal the other individual or be contrary to the national interest.**	**Ensure no one besides the owner or organisation obtains the data with malicious intent.**	**This means that the organisation in charge can withhold information that can be used to threaten, cause harm or reveal the other individual or be contrary to the national interest.**
7	**Personal Data Protection Act Part V**	**22 – Correction of Personal Data (1)**	**An individual may request an organisation to correct an error in the personal data about the individual that is the owner or under the organisation.**	**Ensure that data is up to date as it is managed by the user or the person in charge of the organisation**	**This means that data can be requested if there are any errors or changes to data that needs to be regularly updated by the company or individual.**
8	**Personal Data Protection Act Part V**	**22 – Correction of Personal Data (2)**	**Any authorised person can request a change of data deemed fit.**	**Ensure the person changing the data is the owner by showing verifications.**	**This means if a person is to change any data info, they are supposed to show image identification the same as the data owner.**

9	**Personal Data Protection Act Part VI**	**24 – Protection of Personal Data**	**The organisation must make protect personal data by making reasonable security arrangements.**	**Limit the access to the personal data and lock the data from being accessed by all unless authorised.**	**This means the data obtained by the organisation must be protected to prevent unauthorised access.**

Part D (Access Controls)

Users In groups



HR Properties

General

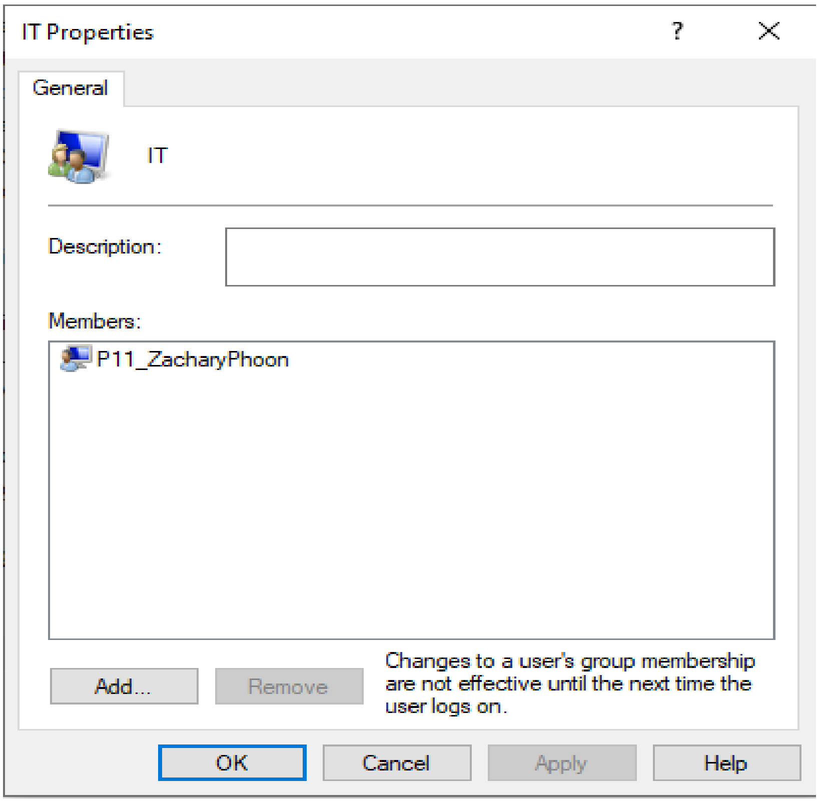
HR

Description:

Members:

Betty

Changes to a user's group membership are not effective until the next time the user logs on.



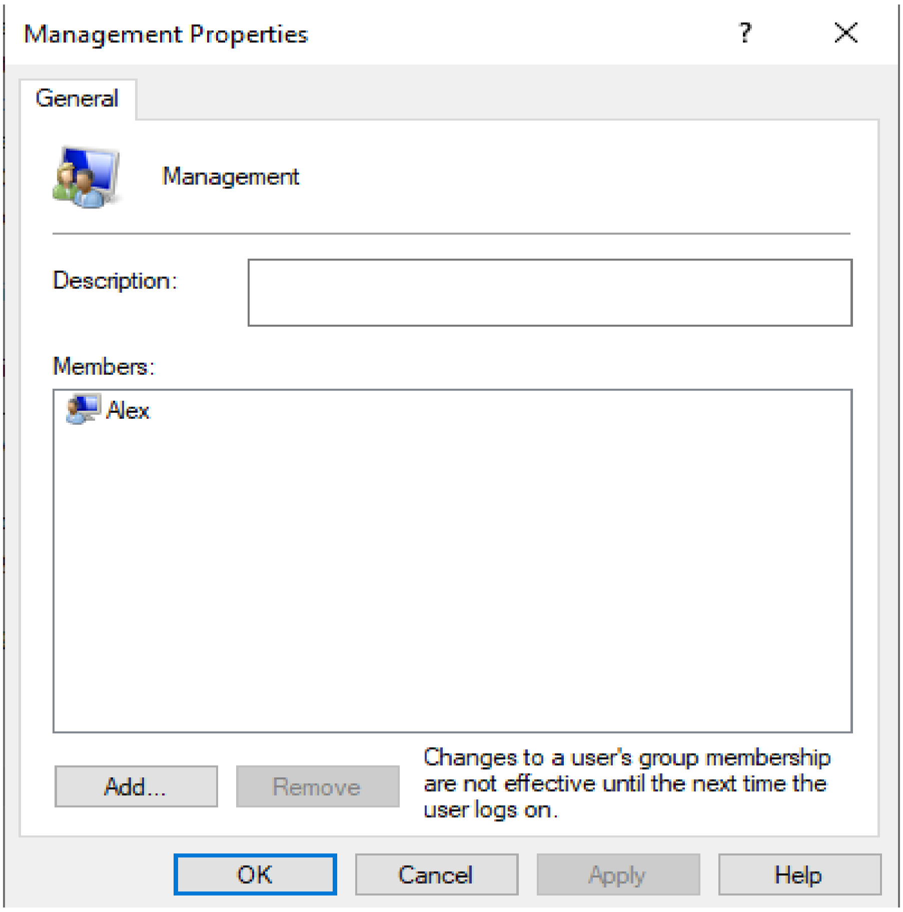
IT

Description:

Members:

P11_ZacharyPhoon

Changes to a user's group membership are not effective until the next time the user logs on.



Management Properties

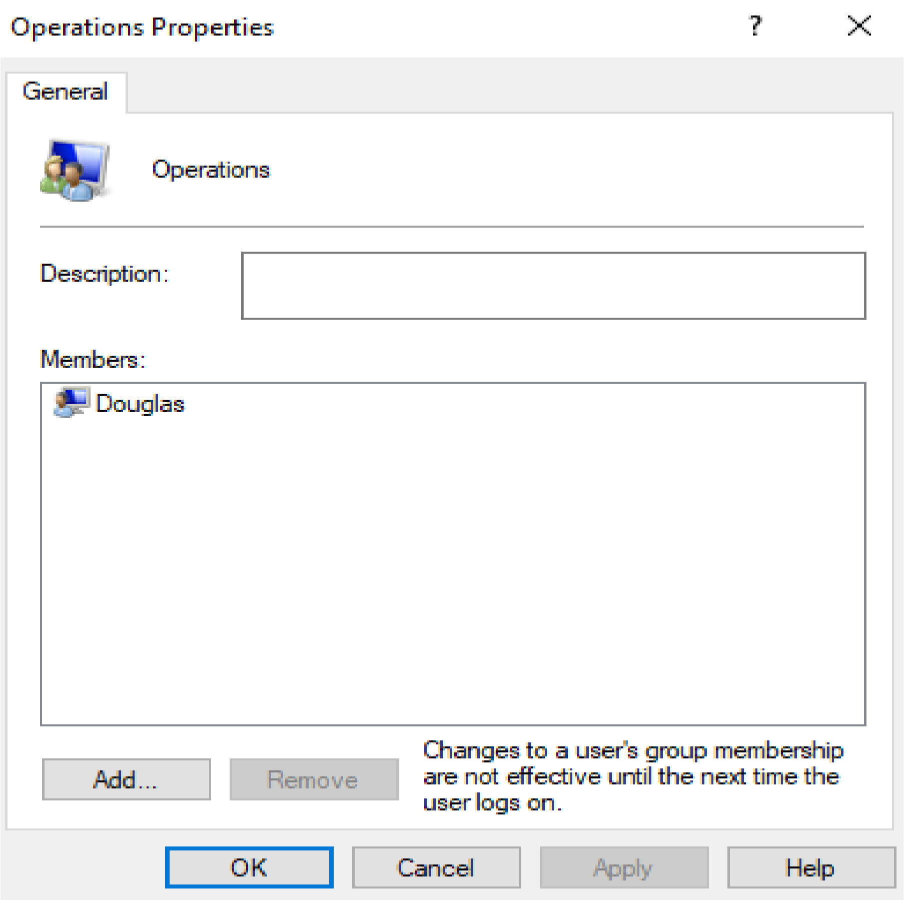
Management

Description:

Members:

Alex

Changes to a user's group membership are not effective until the next time the user logs on.



Operations Properties

Operations

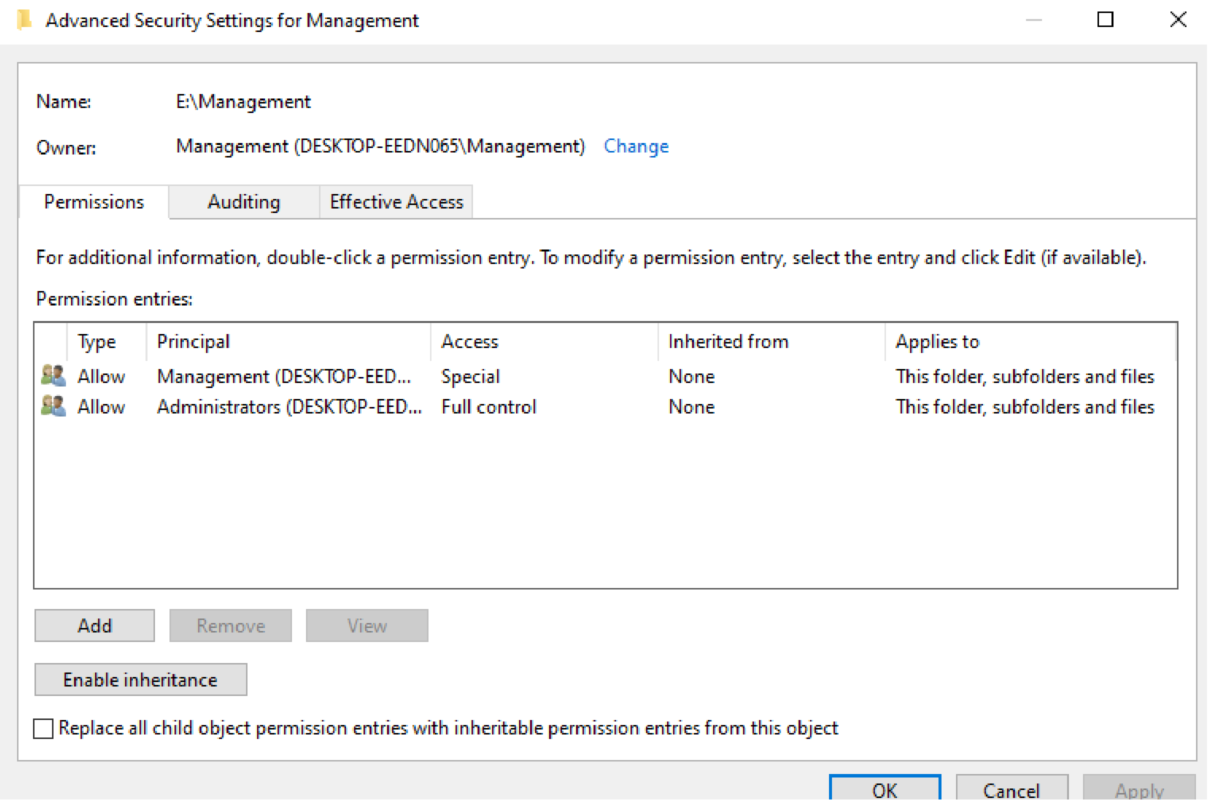
Description:

Members:

Douglas

Changes to a user's group membership are not effective until the next time the user logs on.

Management Folder Access Controls



Name: E:\Management

Owner: Management (DESKTOP-EEDN065\Management)

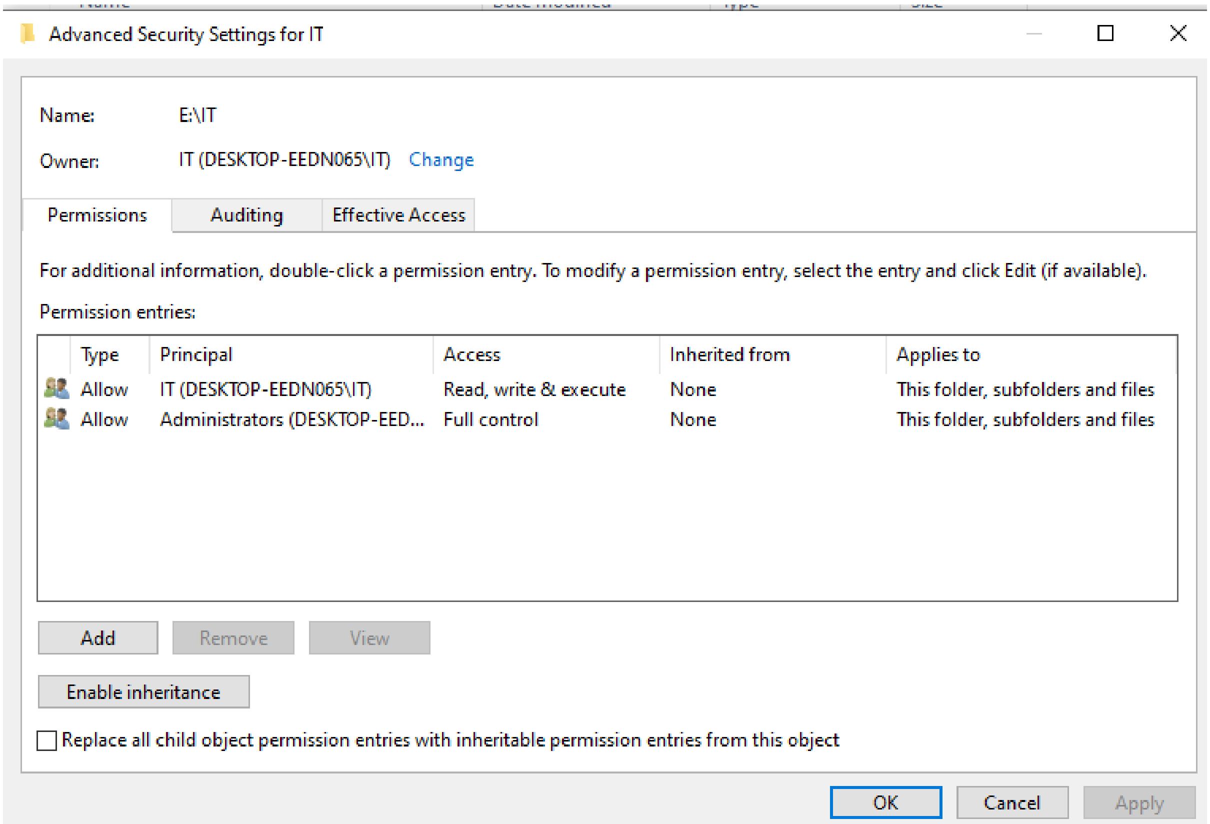
For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	Management (DESKTOP-EED...	Special	None	This folder, subfolders and files
Allow	Administrators (DESKTOP-EED...	Full control	None	This folder, subfolders and files

□ Replace all child object permission entries with inheritable permission entries from this object

IT Folder Access Controls



Name: E:\IT

Owner: IT (DESKTOP-EEDN065\IT)

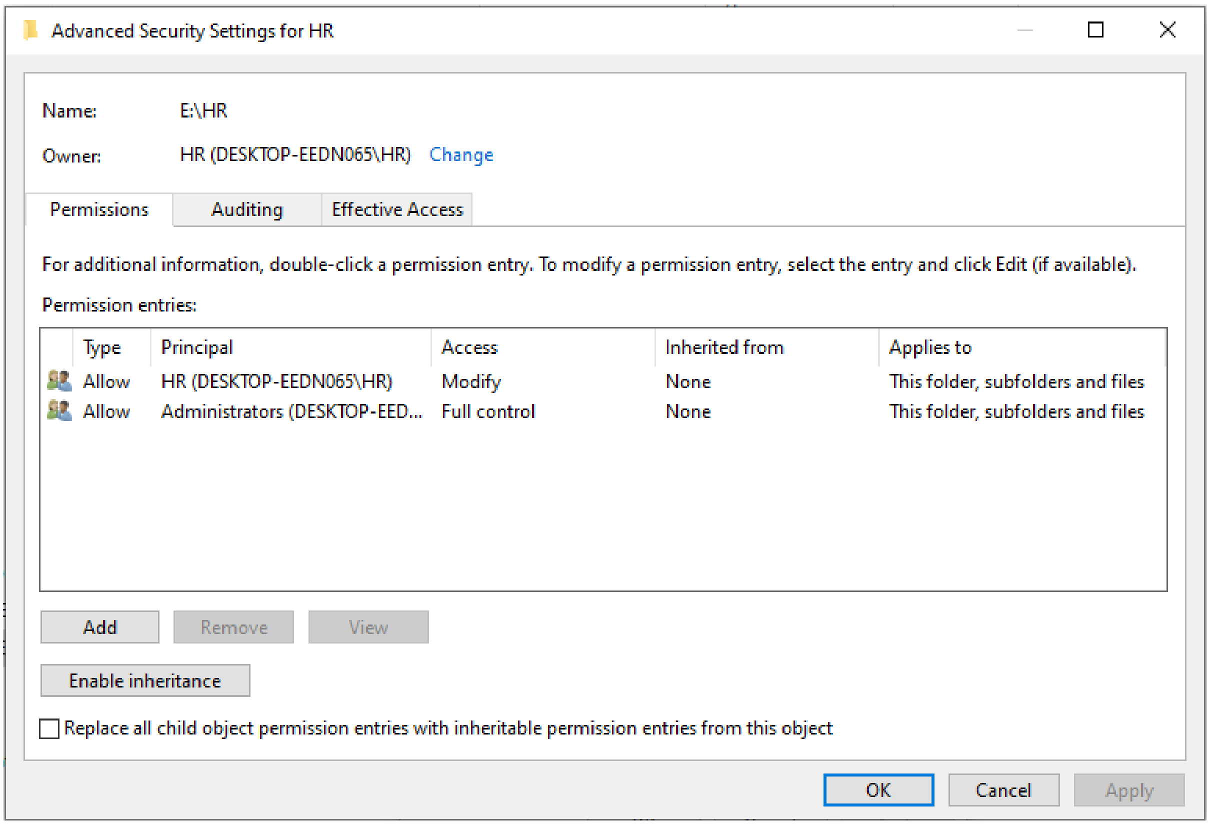
For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	IT (DESKTOP-EEDN065\IT)	Read, write & execute	None	This folder, subfolders and files
Allow	Administrators (DESKTOP-EED...	Full control	None	This folder, subfolders and files

□ Replace all child object permission entries with inheritable permission entries from this object

HR Folder Access Controls



Name: E:\HR

Owner: HR (DESKTOP-EEDN065\HR) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	HR (DESKTOP-EEDN065\HR)	Modify	None	This folder, subfolders and files
Allow	Administrators (DESKTOP-EED...	Full control	None	This folder, subfolders and files

□ Replace all child object permission entries with inheritable permission entries from this object

Suggestions for Physical Access Point

Firstly, Lock Server Rooms with network devices place the server room under surveillance.

Secondly, Fingerprint access to the workplace with technology connected to the network system.

Thirdly, Secure the company printer and add a layer of security for portable devices.

Fourthly, Secure the Backup files and Disable USB ports to prevent any malicious devices from the plugged into the system.

Suggestion for Logical Access Point

Firstly, ensure permissions controls are regularly maintained and updated.

Secondly, implement measures and applications to detect and mitigate malicious software and unauthorised users when accessing info.

Thirdly, give internet services on a different network for users with their won device; this other network will have higher security and protection as it is more vulnerable due to its significant exposure to the internet outside of the workplace.

Part E (End Point Security)

1. Account Policies

-1.0.1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)'

Reason: Prevent reusing a password as if reused, the easier an attacker can brute force attacks.

-1.0.1.1.3 (L1) Ensure 'Minimum password age is set to '1 or more day(s)'

Reason: To prevent possible password reuse when a changing on the same day.

2. Local Policies

-1.0. 2.2.2 (L1) Ensure 'Access this computer from the network' is set to Administrators, Remote Desktop Users

Reason: Users who can connect from their computer to the network can access resources on target computers for which they have permission.

-1.0. 2.2.5 (L1) Ensure 'Allow log on locally' is set to 'Administrators, Users'

Reason: Any account with the “Allow log on locally” user right can log on at the computer’s console, which means unauthorised users can download and run malicious software to elevate their privileges.

5. System Services

-1.0.5.8(L1) Ensure 'Internet Connection Sharing (ICS) (SharedAccess)' is set to 'Disabled'

Reason: This feature causes networks to bridge and likely bypass other, more secure pathways. It should not be used on any enterprise-managed system.

- 1.0. 5.41 (L1) Ensure 'Xbox Accessory Management Service (XboxGipSvc)' is set to 'Disabled.'

Reason: Xbox Live is a gaming service and has no place in an enterprise managed environment (perhaps unless it is a gaming company).

9. Windows Firewall with Advanced Security

-1.0. 9.1.1 (L1) Ensure 'Windows Firewall: Domain: Firewall state, is set to 'On (recommended).'

Reason: If the firewall is turned off, all traffic will be able to access the system, and an attacker may be more easily able to remotely exploit a weakness in a network service.

-1.0. 9.1.2 (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default).'

Reason: If the firewall allows all traffic to access the system, then an attacker may be more easily able to remotely exploit a weakness in a network service.

17. Advance Audit Policy Configuration

-1.0. 17.1.1 (L1) Ensure 'Audit Credential Validation' is set to 'Success and Failure.'

Reason: Auditing these events may be helpful when investigating a security incident.

-1.0. 17.2.1 (L1) Ensure 'Audit Application Group Management' is set to 'Success and Failure.'

Reason: Auditing events in this category may be helpful when investigating an incident.

18. Administrative Templates (Computer)

-1.0. 18.1.1.1 (L1) Ensure 'Prevent enabling lock screen camera' is set to 'Enabled'

Reason: Disabling the lock screen camera extends the protection afforded by the lock screen to camera features

-1.0. 18.1.1.2 (L1) Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled.'

Reason: Disabling the lock screen slide show extends the protection afforded by the lock screen to slide show contents.

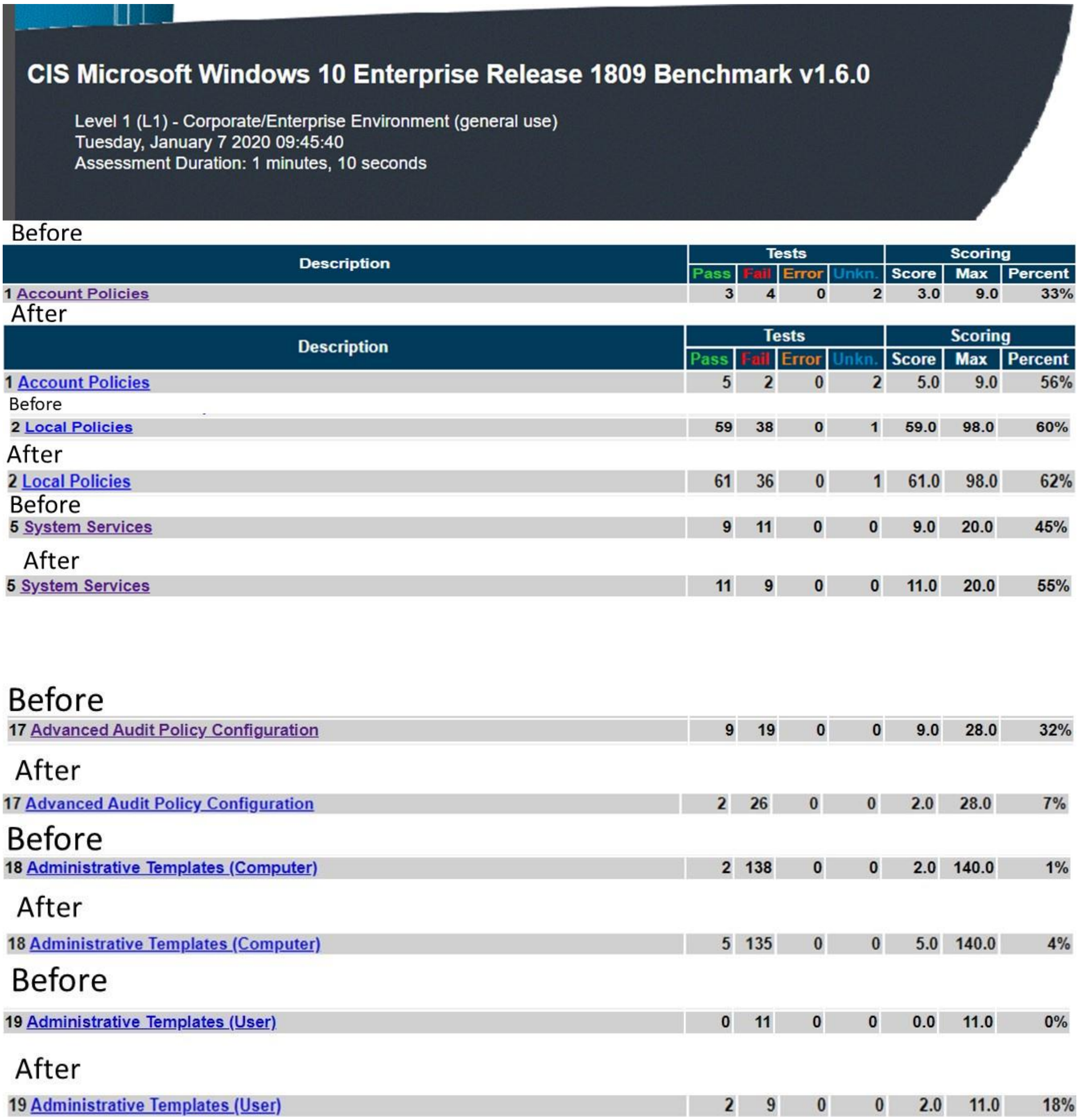
19. Administrative Templates (User)

-1.0. 19.1.3.1 (L1) Ensure 'Enable screen saver' is set to 'Enabled.'

Reason: If a user forgets to lock their computer when they walk away, a passer-by may hijack it. Configuring a timed screen saver with a password lock will help to protect against these hijacks.

-1.0. 19.1.3.2 (L1) Ensure 'Force specific screen saver: Screen saver executable name' is set to 'Enabled: screensaver.screen

Reason: If a user forgets to lock their computer when they walk away, a passer-by may hijack it. Configuring a timed screen saver with a password lock will help to protect against these hijacks.



CIS Microsoft Windows 10 Enterprise Release 1809 Benchmark v1.6.0

Level 1 (L1) - Corporate/Enterprise Environment (general use)
Tuesday, January 7 2020 09:45:40
Assessment Duration: 1 minutes, 10 seconds

Before

Description	Tests				Scoring		
	Pass	Fail	Error	Unkn.	Score	Max	Percent
1 Account Policies	3	4	0	2	3.0	9.0	33%

After

Description	Tests				Scoring		
	Pass	Fail	Error	Unkn.	Score	Max	Percent
1 Account Policies	5	2	0	2	5.0	9.0	56%

Before

2 Local Policies	59	38	0	1	59.0	98.0	60%

After

2 Local Policies	61	36	0	1	61.0	98.0	62%

Before

5 System Services	9	11	0	0	9.0	20.0	45%

After

5 System Services	11	9	0	0	11.0	20.0	55%

Before

17 Advanced Audit Policy Configuration	9	19	0	0	9.0	28.0	32%

After

17 Advanced Audit Policy Configuration	2	26	0	0	2.0	28.0	7%

Before

18 Administrative Templates (Computer)	2	138	0	0	2.0	140.0	1%

After

18 Administrative Templates (Computer)	5	135	0	0	5.0	140.0	4%

Before

19 Administrative Templates (User)	0	11	0	0	0.0	11.0	0%

After

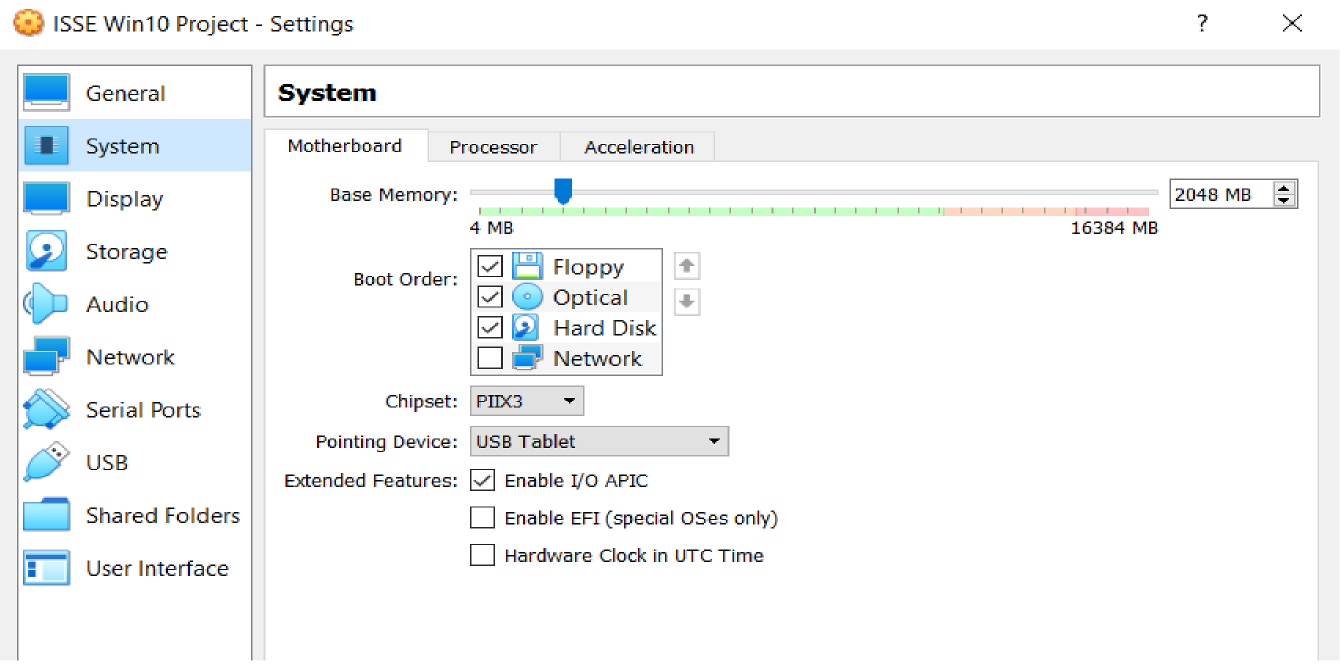
19 Administrative Templates (User)	2	9	0	0	2.0	11.0	18%

Part F (Conclusion)

This comes to the end of this word document regarding the fundamentals of Summary of Operations System, Cyber Security Concept, Computer misuse & Cyber security Act and Data Protection Act. Access controls and Endpoint security. With this detail,, you can now protect us from potential cyberattacks and potential bridge of the network.

Part G (Appendix)

Project Virtual Machine SPECIFICATIONS



Base Memory: 2048 MB

Boot Order:
☑ Floppy
☑ Optical
☑ Hard Disk
☐ Network

Chipset: PIIX3

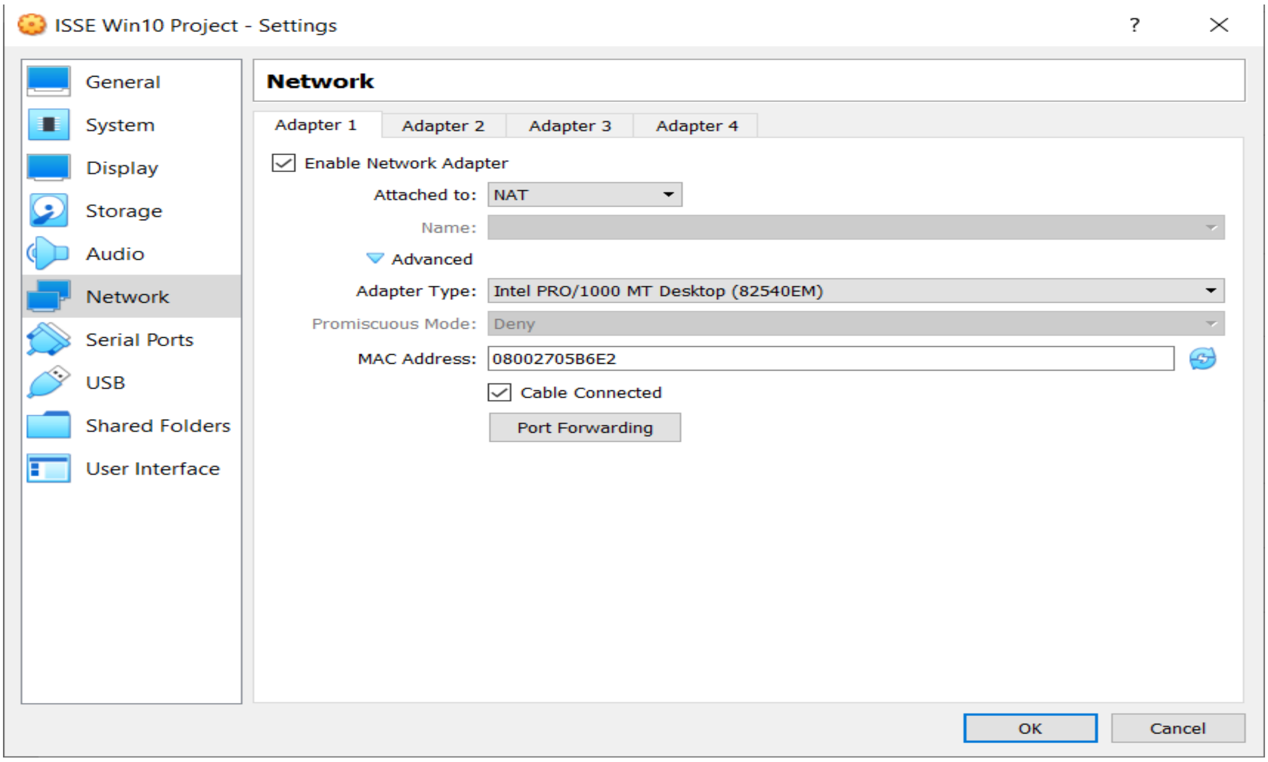
Pointing Device: USB Tablet

Extended Features: ☑ Enable I/O APIC

☐ Enable EFI (special OSes only)

☐ Hardware Clock in UTC Time

The image above shows a Ram of 2048 MB, which is 2GB after conversion.



☑ Enable Network Adapter

Attached to: NAT

Name:

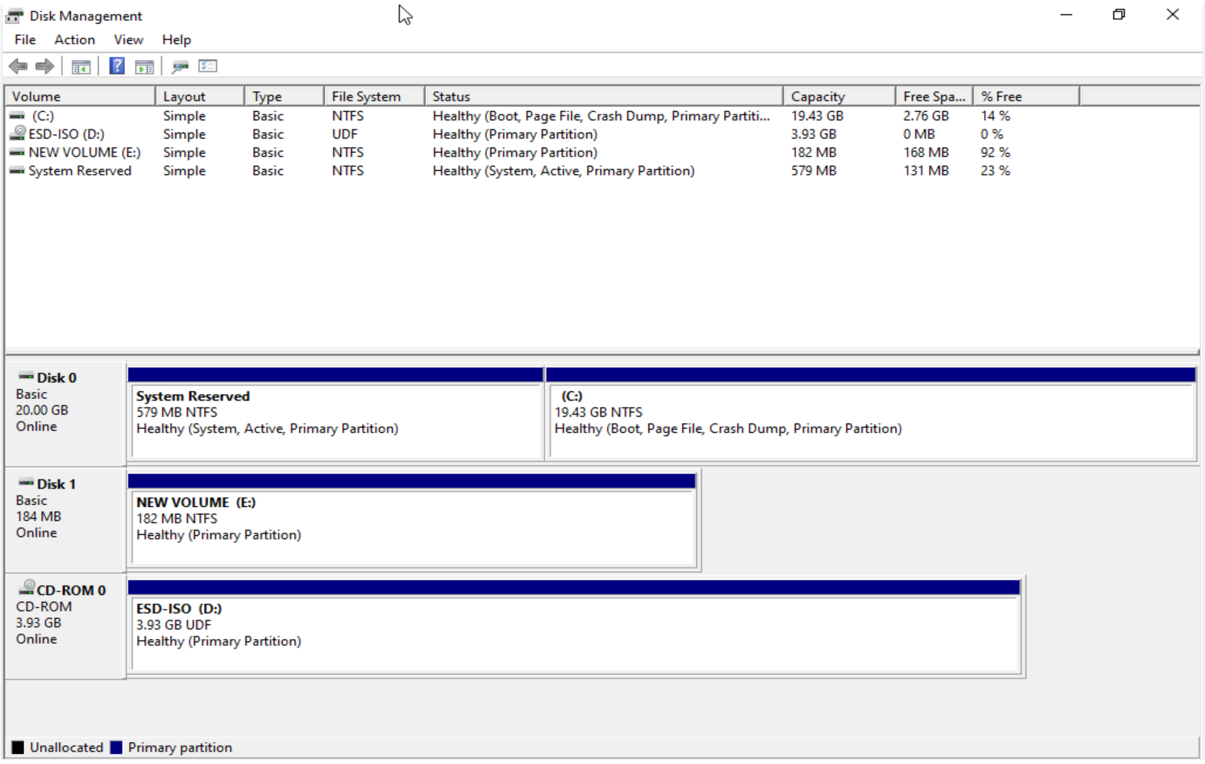
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 08002705B6E2

☑ Cable Connected

The above image is the Virtual Machine's Network adapter, a NAT Ethernet.



Disk Management

File Action View Help

Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partiti...	19.43 GB	2.76 GB	14 %
ESD-ISO (D:)	Simple	Basic	UDF	Healthy (Primary Partition)	3.93 GB	0 MB	0 %
NEW VOLUME (E:)	Simple	Basic	NTFS	Healthy (Primary Partition)	182 MB	168 MB	92 %
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	579 MB	131 MB	23 %

Disk 0
Basic
20.00 GB
Online

System Reserved
579 MB NTFS
Healthy (System, Active, Primary Partition)

(C:)
19.43 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

Disk 1
Basic
184 MB
Online

NEW VOLUME (E:)
182 MB NTFS
Healthy (Primary Partition)

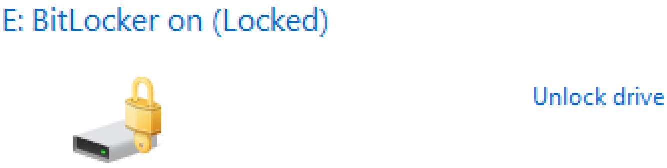
CD-ROM 0
CD-ROM
3.93 GB
Online

ESD-ISO (D:)
3.93 GB UDF
Healthy (Primary Partition)

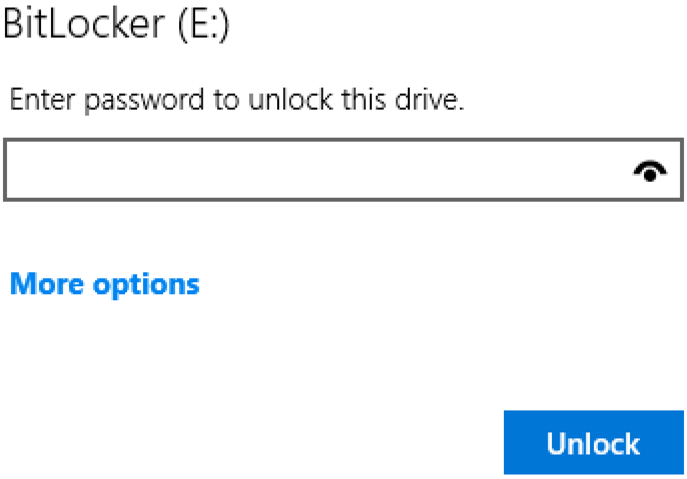
■ Unallocated 🟦 Primary partition

The Above image is the Virtual Machine's Disk memory for the Operating System and the Additional 200MB of storage. C: drive is the disk used for the operating system, and E: drive is to add 200MB of GPT partition.

BLOCKED E: DRIVE



E: BitLocker on (Locked)



BitLocker (E:)

Enter password to unlock this drive.

Part H (References/Acknowledgement)

Personal Data Protection Act :

https://sso.agc.gov.sg/Act/PDPA2012#pr21-

Computer Misuse Act :

https://sso.agc.gov.sg/Act/CMA1993#legis

Cyber Security Act :

https://sso.agc.gov.sg/Act/CA2018