ISRM/IAM Privileged Access Governance Enhancement (PAGE) Project

**Doc. No:** ISRM\_IAM\_PAGE\_DEC\_001

**Title: PAGE Project Governance definition**

|  |  |  |
| --- | --- | --- |
| **Author(s):** |  |  |
| |  |  |  | | --- | --- | --- | | PAGE Project Manager  ISRM/IAM |  |  | |  |  |
| **Approver(s):** |
| Sujoy Ghosh  IAM Lead  ISRM/IAM |  |  |

Gurgen Bakunc

TIS IHS

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Sujoy Ghosh  CIS Performance Engineering  CIS |  |  |
|  |
| Nicholas Balestrino  Application Manager  Sr. Director Workspace Services  TIS- Digital Workspace Svcs |  |  |
| Petr Kozák  BISE  ISRM |  |  |

TIS

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |

**Document History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Comments** |
| 1.0 | 15-Mar-2023 | Gurgen Bakunc | Initial version |

**Convention**

The words “Must (has / have to)”, “Should” and “May / Can” are used as follows:

|  |  |
| --- | --- |
| **Word** | **Definition** |
| **Must:** | This word, or the terms “required” or “shall”, mean that the definition is an absolute requirement of the specification. |
| **Should:** | This term, or the adjective “recommended”, indicates recommendations that are expected to apply unless shown to be inapplicable or replaced by an alternative demonstrated to provide at least an equivalent level of quality and / or security. |
| **May / Can:** | This word, or the adjective “optional”, means that the application of an item is at the discretion of the user. |

**Dates** should be stated in the **form** “dd-mmm-yyyy”, e.g. 01-Aug-2016

**Explanation / Definition of Terms**

The terms and definitions are published in the [IS Glossary](http://igm.novartis.net/IGM_Policy_Framework/Pages/glossary.aspx), accessible via the IS ISRM web page.

**Publication**

This document is published in the ISRM\_IAM\_PAGE - Shared Documents - All Documents (novartis.net).

# Purpose

The purpose of this document is to document new governance for Privileged account agreed as par of PAGE project. The governance was confirmed by ITLT and Cyber SteerCo decision in 2019 and 2020.

# Introduction

The project PAGE will introduce new Governance model for all Privileged account used in Novartis. The governance model and new account types have been reviewed and approved by ITLT and Cyber SteerCo.

# Decision

This decision document defined new account types and responsibilities to use the for all environments used in Novartis. Following documents are attached are include the details:

* **Account Type Definitions** [2] – excel file listing all new account typed that will be supported after application transition
* **PAGE principles overview** [3] – Slide deck presented and approved by Cyber Steerco in January 2020
* **Current access model**
* **PAGE principles implementation to M365\_Platform**

# Roles and Responsibilities

## RACI Summary Table

*Generic description of the WI roles in terms of the overall accountability/responsibility in each of the process activities. We use 4 types:*

*R – Responsibility: Ownership for an activity that needs to be performed in order to deliver an outcome or result; responsibility can be shared or delegated*

*A – Accountability: Ownership for an outcome or a result that needs to be achieved, regardless of conditions; accountability can be neither shared nor delegated*

*C – Consulted: Those whose opinions are sought on an activity (two-way communication)*

*I – Informed: Those who are kept up to date on the progress of an activity (one-way communication)*

### For Onboarding Process

|  |  |  |
| --- | --- | --- |
| **Responsibility** | **AES** | **M365\_Platform** |
| M365\_SHAREPOINT (50231,44205,44104,31727, 33371, 28549, 43489,45906,45831) Maintenance and support | R/A | I |
| Gathering Inputs | A | R |
| Validating Information | R/A | I/C |
| Creating/revoking Users | R/A | I/C |

### For Operation Process – M365\_Platform

M365\_Platform team is required OS previledge access to maintain & support the applications, hence priviledged access delicated to M365\_Platform team.

## Role Description

Roles and accountabilities/responsibilities related to this document are:

| **Role Name** | **Description** |
| --- | --- |
| AES Team | AES team will be responsible on reviewing the information provided by the Application Team. |
| M365\_Platform Team | M365\_Platform team is responsible for timely sharing the details of their applications and providing required support for transition of OS bound privilege. |

# System Overview

Applications are on-boarded to PAGE for security concern to have limited access at a server level.

# Work-Instructions

## PAGE Operations Process

AES team will not be handling any of the operational tasks (Incident, Service request and change request) of SCCM and APP PORTAL as PAGE compliant privileged access is being granted to SCCM and APP PORTAL services team to handle all the privileged tasks themselves. Please refer section 8.2 for account details.

# Current Access Model

## Related applications

Applications related to O365\_Platform Services:

|  |  |
| --- | --- |
| Application ID | Application Name |
| 50231 | Microsoft M365 – Platform (Parent) |
| 33371 | O365 SharePoint Online & OneDrive |
| 44104 | Microsoft Teams |
| 44205 | Azure Information Protection |
| 31727 | Exchange Messaging |
| 43489 | M365 Automatic License Assignment |
| 28549 | eDiscovery Litigation Services – LRMT |
| 45906 | Microsoft M365 Tools & Services (Parent) |
| 45831 | CMMS |

## Accounts and groups owned by O365\_Platform services

| **Account name** | **Group name** | **Use case OS/Appliance Privilege** | | **Azure AD Role (Y/N)** | **Specify the role** | **Application Name & ID** | **Platform team comment** | **Assesment - PAGE** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| SYS\_NOVAODB1 |  |  | Used by O365ALA application to derive data from O365 and assign O365 Licenses. | *Y* | *License Administrator, SharePoint Administrator, Skype for Business Administrator, Teams Administrator, User Administrator* | *ALA (43489)* | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *Acconts can be in application safe but required approved GAP* |
| SYS\_NOVAODB2 |  |  | Used by O365ALA application to derive data from O365 and assign O365 Licenses. | Y | License Administrator, SharePoint Administrator, Skype for Business Administrator, Teams Administrator, User Administrator | *ALA (43489)* | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *Acconts can be in application safe but required approved GAP* |
| SYS\_NOVAODB3 |  |  | Used by O365ALA application to derive data from O365 and assign O365 Licenses. | *Y* | *License Administrator, SharePoint Administrator, Skype for Business Administrator, Teams Administrator, User Administrator* | *ALA (43489)* | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *Acconts can be in application safe but required approved GAP* |
| SYS\_NOVAODB4 |  |  | Used by O365ALA application to derive data from O365 and assign O365 Licenses. | Y | License Administrator, SharePoint Administrator, Skype for Business Administrator, Teams Administrator, User Administrator | *ALA (43489)* | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *Acconts can be in application safe but required approved GAP* |
| SYS\_NOVAODB5 |  |  | Used by O365ALA application to derive data from O365 and assign O365 Licenses. | Y | License Administrator, SharePoint Administrator, Skype for Business Administrator, Teams Administrator, User Administrator | *ALA (43489)* | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *Acconts can be in application safe but required approved GAP* |
| SYS\_NOVAODB6 |  |  | Used by O365ALA application to derive data from O365 and assign O365 Licenses. | Y | License Administrator, SharePoint Administrator, Skype for Business Administrator, Teams Administrator, User Administrator | *ALA (43489)* | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *Acconts can be in application safe but required approved GAP* |
| SYS\_NOVAODB7 |  |  | Used by O365ALA application to derive data from O365 and assign O365 Licenses. | Y | License Administrator, SharePoint Administrator, Skype for Business Administrator, Teams Administrator, User Administrator | *ALA (43489)* | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *Acconts can be in application safe but required approved GAP* |
| SYS\_NOVAODB8 |  |  | Used by O365ALA application to derive data from O365 and assign O365 Licenses. | Y | License Administrator, SharePoint Administrator, Skype for Business Administrator, Teams Administrator, User Administrator | *ALA (43489)* | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *Acconts can be in application safe but required approved GAP* |
| SYS\_NOVAODB9 |  |  | Used by O365ALA application to derive data from O365 and assign O365 Licenses. | Y | License Administrator, SharePoint Administrator, Skype for Business Administrator, Teams Administrator, User Administrator | *ALA (43489)* | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *Acconts can be in application safe but required approved GAP* |
| SYS\_NOVAODB10 |  |  | Used by O365ALA application to derive data from O365 and assign O365 Licenses. | Y | License Administrator, SharePoint Administrator, Skype for Business Administrator, Teams Administrator, User Administrator | *ALA (43489)* | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *Acconts can be in application safe but required approved GAP* |
| SYS\_NOVARODB |  |  | Account under which O365ALA Scheduled Tasks and Application runs under. | Y | License Administrator, SharePoint Administrator, Skype for Business Administrator, Teams Administrator, User Administrator | *ALA (43489)* | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *Acconts can be in application safe but required approved GAP* |
| TEC\_NOVARODB1 |  |  | Used to access LRMT and O365 ALA Servers for troubleshooting. | N |  | LRMT (28549) | This requires review with the technical team if the ownership could be handed over to PAGE and replace with App / JIT accounts. | This account remain the same as they need this account for trobleshoting purpose & this account also connected with DB which is in frequent use. |
| TEC\_LCMSCHED |  |  | Used to access LRMT and O365 ALA Servers for troubleshooting and the account under which LCM Scheduled Tasks run under. | N |  | LRMT (28549) | This requires review with the technical team if the ownership could be handed over and replace with App / JIT accounts. | This account can be replaced with sys account in order to run the services. |
| TEC\_LCMAPPLI |  |  | Account under which LCM Application runs under. | N |  | LRMT (28549) | This requires review with the technical team if the ownership could be handed over and replace with App / JIT accounts. | As this account is no longer required hence it can be revoked. |
| TEC\_LRMTPRE1 |  |  | Account used by LRMT Preservation Module for accessing MS Compliance Center, Exchange Online and SharePoint Online | Y | Compliance Administrator, License Administrator, SharePoint Administrator, User Administrator | LRMT (28549) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_LRMTPRE2 |  |  | Account used by LRMT Preservation Module for accessing MS Compliance Center, Exchange Online and SharePoint Online | Y | Compliance Administrator, License Administrator, SharePoint Administrator, User Administrator | LRMT (28549) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_LRMTPRE3 |  |  | Account used by LRMT Preservation Module for accessing MS Compliance Center, Exchange Online and SharePoint Online | Y | Compliance Administrator, License Administrator, SharePoint Administrator, User Administrator | LRMT (28549) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_LRMTPRE4 |  |  | Account used by LRMT Preservation Module for accessing MS Compliance Center, Exchange Online and SharePoint Online | Y | Compliance Administrator, License Administrator, SharePoint Administrator, User Administrator | LRMT (28549) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_LRMTPRE5 |  |  | Account used by LRMT Preservation Module for accessing MS Compliance Center, Exchange Online and SharePoint Online | Y | Compliance Administrator, License Administrator, SharePoint Administrator, User Administrator | LRMT (28549) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_LRMTPRE6 |  |  | Account used by LRMT Preservation Module for accessing MS Compliance Center, Exchange Online and SharePoint Online | Y | Compliance Administrator, License Administrator, SharePoint Administrator, User Administrator | LRMT (28549) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_NOVARED1 |  |  | Account used by eDLS Team to access MS eDiscovery Compliance Center and Exchange Online  This ID is used to access to multiple servers when running various scripts, copying data via RoboCopy, querying data across multiple databases across multiple servers and exporting data from External MS Applications – currently we use TEC accounts that have access rights across many servers. | Y | eDiscovery Manager | LRMT (28549) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_NOVARED2 |  |  | Account used by eDLS Team to access MS eDiscovery Compliance Center and Exchange Online  This ID is used to access to multiple servers when running various scripts, copying data via RoboCopy, querying data across multiple databases across multiple servers and exporting data from External MS Applications – currently we use TEC accounts that have access rights across many servers. | Y | eDiscovery Manager | LRMT (28549) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_NOVARED3 |  |  | Account used by eDLS Team to access MS eDiscovery Compliance Center and Exchange Online  This ID is used to access to multiple servers when running various scripts, copying data via RoboCopy, querying data across multiple databases across multiple servers and exporting data from External MS Applications – currently we use TEC accounts that have access rights across many servers. | Y | eDiscovery Manager | LRMT (28549) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_NOVARED4 |  |  | Account used by eDLS Team to access MS eDiscovery Compliance Center and Exchange Online  This ID is used to access to multiple servers when running various scripts, copying data via RoboCopy, querying data across multiple databases across multiple servers and exporting data from External MS Applications – currently we use TEC accounts that have access rights across many servers. | Y | eDiscovery Manager | LRMT (28549) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_NOVARED5 |  |  | Account used by eDLS Team to access MS eDiscovery Compliance Center and Exchange Online  This ID is used to access to multiple servers when running various scripts, copying data via RoboCopy, querying data across multiple databases across multiple servers and exporting data from External MS Applications – currently we use TEC accounts that have access rights across many servers. | Y | eDiscovery Manager | LRMT (28549) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_NOVARED6 |  |  | Account used by eDLS Team to access MS eDiscovery Compliance Center and Exchange Online  This ID is used to access to multiple servers when running various scripts, copying data via RoboCopy, querying data across multiple databases across multiple servers and exporting data from External MS Applications – currently we use TEC accounts that have access rights across many servers. | Y | eDiscovery Manager | LRMT (28549) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_NOVARED7 |  |  | Account used by eDLS Team to access MS eDiscovery Compliance Center and Exchange Online  This ID is used to access to multiple servers when running various scripts, copying data via RoboCopy, querying data across multiple databases across multiple servers and exporting data from External MS Applications – currently we use TEC accounts that have access rights across many servers. | Y | eDiscovery Manager | LRMT (28549) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_NOVARED8 |  |  | Account used by eDLS Team to access MS eDiscovery Compliance Center and Exchange Online  This ID is used to access to multiple servers when running various scripts, copying data via RoboCopy, querying data across multiple databases across multiple servers and exporting data from External MS Applications – currently we use TEC accounts that have access rights across many servers. | Y | eDiscovery Manager | LRMT (28549) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_O365SVCACC01 |  |  | Global M365 Account. | Y | Company Administrator  TenantAdmins | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_O365SVCACC02 |  |  | Account used for Managing Tenant level activities. Also the account used for several automation solutions. | Y | Groups Administrator  Office Apps Administrator  Power BI Administrator  Power Platform Administrator  SharePoint Administrator  Teams Administrator  User Administrator  UserAccountAdmins | O365 SharePoint Online & OneDrive  (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_O365SVCACC03 |  |  | Account used for Managing Tenant level activities. Also the account used for several automation solutions. | Y | Groups Administrator  Office Apps Administrator  Power BI Administrator  Power Platform Administrator  SharePoint Administrator  Teams Administrator  User Administrator  UserAccountAdmins | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_O365SVCACC04 |  |  | Account used to manage the MS Teams administration with the devices. | Y | Teams Devices Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_O365SVCACC05 |  |  | Accounts used to login to dev, QA, Production servers. | N |  | O365 SharePoint Online & OneDrive (33371) | Account being reviewed for decommission | Can be revoked |
| TEC\_O365SVCACC06 |  |  | Accounts used to login to dev, QA, Production servers. | N |  | O365 SharePoint Online & OneDrive (33371) | Account being reviewed for decommission | Can be revoked |
| TEC\_O365SVCACC07 |  |  | Accounts used to login to dev, QA, Production servers. | N |  | O365 SharePoint Online & OneDrive (33371) | Account being reviewed for decommission | Can be revoked |
| ADM\_PPADMIN1 |  |  | Account used to login to dev, QA, production servers. Also this account is used by operations team to work on the operation activities. | Y | SharePoint Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be replaced with Tec account with similar role |
| ADM\_PPADMIN2 |  |  | Account used to login to dev, QA, production servers. Also this account is used by operations team to work on the operation activities. | Y | SharePoint Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be replaced with Tec account with similar role |
| ADM\_PPADMIN3 |  |  | Account used to login to dev, QA, production servers. Also this account is used by operations team to work on the operation activities. | Y | SharePoint Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be replaced with Tec account with similar role |
| ADM\_PPADMIN4 |  |  | Account used to login to dev, QA, production servers. Also this account is used by operations team to work on the operation activities. | Y | SharePoint Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be replaced with Tec account with similar role |
| ADM\_PPADMIN5 |  |  | Account used to login to dev, QA, production servers. Also this account is used by operations team to work on the operation activities. | Y | SharePoint Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be replaced with Tec account with similar role |
| ADM\_PPADMIN6 |  |  | Account used to login to dev, QA, production servers. Also this account is used by operations team to work on the operation activities. | Y | SharePoint Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be replaced with Tec account with similar role |
| ADM\_PPADMIN7 |  |  | Account used to login to dev, QA, production servers. Also this account is used by operations team to work on the operation activities. | Y | SharePoint Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be replaced with Tec account with similar role |
| ADM\_PPADMIN8 |  |  | Account used to login to dev, QA, production servers. Also this account is used by operations team to work on the operation activities. | Y | SharePoint Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be replaced with Tec account with similar role |
| ADM\_PPADMIN9 |  |  | Account used to login to dev, QA, production servers. Also this account is used by operations team to work on the operation activities. | Y | SharePoint Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be replaced with Tec account with similar role |
| TEC\_M365AdmAcc01 |  |  | Account used for managing and administrating PowerPlatform. | Y | Groups Administrator  Power Platform Administrator  SharePoint Administrator  Teams Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_M365AdmAcc02 |  |  | Account used for managing and administrating PowerPlatform. | Y | Groups Administrator  Power Platform Administrator  SharePoint Administrator  Teams Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| SYS\_SPOAdmin1 |  |  | Account is used for managing and administrating the SharePoint/OneDrive services. Also it is used for User management activities e.g. Guest user off-boarding. | Y | O365 Super Administrator (Collective admin roles and lesser than Global Admin). | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *Acconts can be in application safe but required approved GAP* |
| ADM\_SPOADAD1 |  |  | Account is used for quering unified logs to run automation solutions. | Y | SharePoint Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be replaced with Tec account with similar role |
| ADM\_SPOADAD2 |  |  | Account is used for quering unified logs to run automation solutions. | Y | SharePoint Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be replaced with Tec account with similar role |
| ADM\_SPOADAD3 |  |  | Account is used for quering unified logs to run automation solutions. | Y | SharePoint Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be replaced with Tec account with similar role |
| ADM\_SPOADAD4 |  |  | Account is used for quering unified logs to run automation solutions. | Y | SharePoint Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *This account will be replaced with Tec account with similar role* |
| ADM\_SPOADAD5 |  |  | Account is used for quering unified logs to run automation solutions. | Y | SharePoint Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *This account will be replaced with Tec account with similar role* |
| TEC\_AIPADM01 |  |  | AIP owned account, used by AIP Team for performing AIP Admin activities like Label/Policy creation/updation, log collection, execution of Advanced setting command using powershell , script enhancements, debugging and testing scripts (if needed). | Y | Azure Information Protection administrator.  Sensitivity Label Administrator, Security Reader & View-Only Audit Logs in EXO | Azure Information Protection (44205) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *This account will be retained as they have Azure AD role.* |
| TEC\_AIPADM02 |  |  | AIP owned account which is currently performing AIP encryption for OCD Carbon solution. Currently the page transition is ongoing for carbon OCD and this account will be used and owned by AIP team only, as Carbon OCD solution will be transitioned to page AES team, and they will be using separate account. | Y | Azure Information Protection administrator &  Sensitivity Label Administrator | Azure Information Protection  (44205) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role |
| TEC\_AIPDEV |  |  | On AIP Database server,this account is used for Scheduled Task called ‘Run AIP GMT Import’ – which runs the PowerShell script called AIPGMT.ps1.Script adds the license user automatically to GMT groups scoped under Global policy. Going forward, it may also be used in ADP (Automatic Decryption Process). | N |  | Azure Information Protection  (44205) | Mukesh had informed that it should not be transitioned to PAGE as we will have dependency on PAGE Team for testing / troubleshooting purpose as we will have to raise request with them for this so that they can do screenshare session. This is because safe of account will be owned by them if we decide to transition this account. | *This account will be retained as they have Azure AD role.* |
| TEC\_AIPSU01 |  |  | Super User role is assigned to this account. Used by AIP Team for performing decryption activities of files and PST.Currently,this account is being used for Automatic Decryption Process (ADP). | N |  | Azure Information Protection  (44205) | Cannot be handed over to PAGE due to high risk Platform level permissions which can unecrypt any data and scoped under Platform use. | This account can be retained. |
| TEC\_AIPSU02 |  |  | Super User role is assigned to this account. Used by AIP Team for performing decryption activities of files and PST. Going forward, it may also be used in ADP (Automatic Decryption Process). | N |  | Azure Information Protection  (44205) | Cannot be handed over to PAGE due to high risk Platform level permissions which can unecrypt any data and scoped under Platform use. | This account can be retained. |
| TEC\_AIPLOG1 |  |  | This account is used in the script running on server GLCHBS-SP321007 for collecting AIP logs.Also, used to take RDP, scheduled task execution and troubleshooting script issues. | N |  | Azure Information Protection  (44205) | This account can’t be transitioned to PAGE Team as we will have dependency on them for raising request and screen sharing for any troubleshooting / debugging purpose. This is because the safe of account will be transitioned to them and we will not be able to see it in PAM. | Scheduled task can be operated through sys accounts hence this can be replaced with sys accounts. |
| SYS\_AIPLOSY1 |  |  | Used to logon to AIP Service and get / download user logs on server, GLCHBS-SP321007 which is later forwarded to Splunk. | Y | Azure Information Protection Administrator role | Azure Information Protection  (44205) | This account cannot be transferred to PAGE Team as it has cloud role assigned. | This account can be retained. |
| SYS\_AIPLOG1 |  |  | Alias in PAM is eunet/sys\_aiplog1 and username is sys\_aiplosy1, hence this is same account as SYS\_AIPLOSY1. Used to logon to AIP Service and get / download user logs on server, GLCHBS-SP321007 which is later forwarded to Splunk. | Y | Azure Information Protection Administrator role | Azure Information Protection  (44205) | This account cannot be transferred to PAGE Team as it has cloud role assigned. | This account can be retained |
| SYS\_AIPSU1 |  |  | Super User role was assigned to this account. It was used by AIP Team for performing decryption activities of files and PST. | N |  | Azure Information Protection  (44205) | This is our old super user account which is not in use now | Can be revoked |
| SYS\_AIPSU2 |  |  | Super User role was assigned to this account. It was used by AIP Team for performing decryption activities of files and PST. | N |  | Azure Information Protection  (44205) | This is our old super user account which is not in use now | Can be revoked |
| ADM\_NBNRA1 |  |  | ADM account of Ramesh NBN. | N |  | Azure Information Protection  (44205) | This is not a privileged account and should not be transferred to PAGE Team in transition. Access from server, GLCHBS-SP320603 can be removed. | Replace with App domain account. |
| DHUSIGA1 |  |  |  | N |  | Azure Information Protection  (44205) | This is not a privileged account and should not be transferred to PAGE Team in transition. This account belongs to Gaurav Dhusia. Access from server, GLCHBS-SP320603 can be removed. | Personal accounts are not allowded and will be revoked. |
| PATOUMO1 |  |  |  | N |  | Azure Information Protection  (44205) | This is not a privileged account and should not be transferred to PAGE Team in transition. Access from server, GLCHBS-SP320603 can be removed. | Personal accounts are not allowded and will be revoked. |
| APP01 |  |  | Local account for production server, GLCHBS-SP320603, GLCHBS-SP320791, GLCHBS-SP360211, FANET / PPE server, GLCHBS-SP320820 and server, GLCHBS-ST320491 (this server is showing as retired in SNOW) | N |  | Azure Information Protection  (44205) | Since they are not privileged account as per PAGE Team, it’s not subjected to transition. | Can be revoked |
| APP02 |  |  | Local account for production server, GLCHBS-SP320603, GLCHBS-SP320791, GLCHBS-SP360211, FANET / PPE server, GLCHBS-SP320820 and server, GLCHBS-ST320491 (this server is showing as retired in SNOW) | N |  | Azure Information Protection  (44205) | Since they are not privileged account as per PAGE Team, it’s not subjected to transition. | Can be revoked. |
| TSP\_TO365T3G |  |  | FANET account, which was used to login to pre-production server, GLCHBS-SP320820 to perform super user activities and production server, GLCHBS-SP320603 | N |  | Azure Information Protection  (44205) | Since FANET / PPE domain is already decommissioned, no action is required for this account. | Can be revoked. |
| TEC\_0365LSA2 |  |  | Used to login to Teams powershell and Teams admin center. | Y | Reports Reader;  Service Support Administrator;  Skype for Business Administrator;  Teams Administrator;  Teams Communications Administrator;  Teams Communications Support Engineer;  Team Communications Support Specialist;  ServiceSupportAdmins | Microsoft Teams (44104) | Cannot be handed over to PAGE due to high risk Platform level permissions. | This account can be retained. |
| TEC\_MESSASU2  TEC\_MESSASU3  TEC\_MESSASU4  TEC\_MESSASU5  TEC\_MESSASU6  TEC\_MESSASU7  TEC\_MESSASU8  TEC\_MESSASU9 |  |  | Accounts used by Messaging L2 operations team | N |  | Exchange Messaging (31727) | This requires review with the technical team if the ownership could be handed over and replace with App / JIT accounts. | This account can be retained. |
| TEC\_COREMOP1  TEC\_COREMOP2 |  |  | Accounts used by Messaging L4 operations team | Y | Exchange Online (Organization Configuration) | Exchange Messaging (31727) | Cannot be handed over to PAGE due to high risk Platform level permissions. | This account can be retained. |
| TEC\_COREMOP4  TEC\_COREMOP5  TEC\_COREMOP6  TEC\_COREMOP7  TEC\_COREMOP8 |  |  | Accounts used by Messaging L4 operations team and M&A | Y | Exchange Online  License Administrator | Exchange Messaging (31727) | Cannot be handed over to PAGE due to high risk Platform level permissions. | This account can be retained. |
| TEC\_COREMCS3  TEC\_COREMCS4  TEC\_COREMIS2  TEC\_COREMVI1 |  |  | Account used by Corporate Security, ISRM and VIP Support | N |  | Exchange Messaging (31727) | To be discussed with ISRM. | This account can be retained. |

# PAGE principles implementation to O365\_SHAREPOINT

New access model according to PAGE access segregation and account type definission PAGE [2] of the accounts, purpose and ownership.

## Access to 45857 “Commvault - CIS Backup and Restore Services” and CIs under legal data hold

| **Account name** | **Group name** | **Use case OS/Appliance Privilege** | | | **Assesment - PAGE** |
| --- | --- | --- | --- | --- | --- |
| **APP** local account | Local user | Logon to O365\_SHAREPOINT Servers | RDP |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| JIT\_ (Domain Account) | Local Administrators | Just in time priveleged access for O365\_SHAREPOINT team in case the requaed activity is out of AES capability or competence | AES acts as approver – O365\_SHAREPOINT acsts as a user.  Applicable on all servers hosting applications O365\_Sharepoint | Applicable on all servers hosting O365\_Sharepoint applications |  |
| SOS\_ (Domain Account) | Local Administrators | Emergency access in case of major incident | SA team will be the responsible for SOS approvals | Applicable on all servers hosting O365\_Sharepoint applications |  |

## Access to OS bounded Core O365\_Sharepoint servers

| **Account name** | **Group name** | **Use case OS/Appliance Privilege** | | **Azure AD Role (Y/N)** | **Specify the role** | **Application Name & ID** | **Platform team comment** | **Assesment - PAGE** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| SYS\_NOVAODB1 |  |  | Used by O365ALA application to derive data from O365 and assign O365 Licenses. | *Y* | *License Administrator, SharePoint Administrator, Skype for Business Administrator, Teams Administrator, User Administrator* | *ALA (43489)* | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *Acconts can be in application safe but required approved GAP* |
| SYS\_NOVAODB2 |  |  | Used by O365ALA application to derive data from O365 and assign O365 Licenses. | Y | License Administrator, SharePoint Administrator, Skype for Business Administrator, Teams Administrator, User Administrator | *ALA (43489)* | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *Acconts can be in application safe but required approved GAP* |
| SYS\_NOVAODB3 |  |  | Used by O365ALA application to derive data from O365 and assign O365 Licenses. | *Y* | *License Administrator, SharePoint Administrator, Skype for Business Administrator, Teams Administrator, User Administrator* | *ALA (43489)* | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *Acconts can be in application safe but required approved GAP* |
| SYS\_NOVAODB4 |  |  | Used by O365ALA application to derive data from O365 and assign O365 Licenses. | Y | License Administrator, SharePoint Administrator, Skype for Business Administrator, Teams Administrator, User Administrator | *ALA (43489)* | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *Acconts can be in application safe but required approved GAP* |
| SYS\_NOVAODB5 |  |  | Used by O365ALA application to derive data from O365 and assign O365 Licenses. | Y | License Administrator, SharePoint Administrator, Skype for Business Administrator, Teams Administrator, User Administrator | *ALA (43489)* | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *Acconts can be in application safe but required approved GAP* |
| SYS\_NOVAODB6 |  |  | Used by O365ALA application to derive data from O365 and assign O365 Licenses. | Y | License Administrator, SharePoint Administrator, Skype for Business Administrator, Teams Administrator, User Administrator | *ALA (43489)* | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *Acconts can be in application safe but required approved GAP* |
| SYS\_NOVAODB7 |  |  | Used by O365ALA application to derive data from O365 and assign O365 Licenses. | Y | License Administrator, SharePoint Administrator, Skype for Business Administrator, Teams Administrator, User Administrator | *ALA (43489)* | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *Acconts can be in application safe but required approved GAP* |
| SYS\_NOVAODB8 |  |  | Used by O365ALA application to derive data from O365 and assign O365 Licenses. | Y | License Administrator, SharePoint Administrator, Skype for Business Administrator, Teams Administrator, User Administrator | *ALA (43489)* | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *Acconts can be in application safe but required approved GAP* |
| SYS\_NOVAODB9 |  |  | Used by O365ALA application to derive data from O365 and assign O365 Licenses. | Y | License Administrator, SharePoint Administrator, Skype for Business Administrator, Teams Administrator, User Administrator | *ALA (43489)* | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *Acconts can be in application safe but required approved GAP* |
| SYS\_NOVAODB10 |  |  | Used by O365ALA application to derive data from O365 and assign O365 Licenses. | Y | License Administrator, SharePoint Administrator, Skype for Business Administrator, Teams Administrator, User Administrator | *ALA (43489)* | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *Acconts can be in application safe but required approved GAP* |
| SYS\_NOVARODB |  |  | Account under which O365ALA Scheduled Tasks and Application runs under. | Y | License Administrator, SharePoint Administrator, Skype for Business Administrator, Teams Administrator, User Administrator | *ALA (43489)* | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *Acconts can be in application safe but required approved GAP* |
| TEC\_NOVARODB1 |  |  | Used to access LRMT and O365 ALA Servers for troubleshooting. | N |  | LRMT (28549) | This requires review with the technical team if the ownership could be handed over to PAGE and replace with App / JIT accounts. | This account remain the same as they need this account for trobleshoting purpose & this account also connected with DB which is in frequent use. |
| TEC\_LCMSCHED |  |  | Used to access LRMT and O365 ALA Servers for troubleshooting and the account under which LCM Scheduled Tasks run under. | N |  | LRMT (28549) | This requires review with the technical team if the ownership could be handed over and replace with App / JIT accounts. | This account can be replaced with sys account in order to run the services. |
| TEC\_LCMAPPLI |  |  | Account under which LCM Application runs under. | N |  | LRMT (28549) | This requires review with the technical team if the ownership could be handed over and replace with App / JIT accounts. | As this account is no longer required hence it can be revoked. |
| TEC\_LRMTPRE1 |  |  | Account used by LRMT Preservation Module for accessing MS Compliance Center, Exchange Online and SharePoint Online | Y | Compliance Administrator, License Administrator, SharePoint Administrator, User Administrator | LRMT (28549) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_LRMTPRE2 |  |  | Account used by LRMT Preservation Module for accessing MS Compliance Center, Exchange Online and SharePoint Online | Y | Compliance Administrator, License Administrator, SharePoint Administrator, User Administrator | LRMT (28549) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_LRMTPRE3 |  |  | Account used by LRMT Preservation Module for accessing MS Compliance Center, Exchange Online and SharePoint Online | Y | Compliance Administrator, License Administrator, SharePoint Administrator, User Administrator | LRMT (28549) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_LRMTPRE4 |  |  | Account used by LRMT Preservation Module for accessing MS Compliance Center, Exchange Online and SharePoint Online | Y | Compliance Administrator, License Administrator, SharePoint Administrator, User Administrator | LRMT (28549) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_LRMTPRE5 |  |  | Account used by LRMT Preservation Module for accessing MS Compliance Center, Exchange Online and SharePoint Online | Y | Compliance Administrator, License Administrator, SharePoint Administrator, User Administrator | LRMT (28549) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_LRMTPRE6 |  |  | Account used by LRMT Preservation Module for accessing MS Compliance Center, Exchange Online and SharePoint Online | Y | Compliance Administrator, License Administrator, SharePoint Administrator, User Administrator | LRMT (28549) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_NOVARED1 |  |  | Account used by eDLS Team to access MS eDiscovery Compliance Center and Exchange Online  This ID is used to access to multiple servers when running various scripts, copying data via RoboCopy, querying data across multiple databases across multiple servers and exporting data from External MS Applications – currently we use TEC accounts that have access rights across many servers. | Y | eDiscovery Manager | LRMT (28549) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_NOVARED2 |  |  | Account used by eDLS Team to access MS eDiscovery Compliance Center and Exchange Online  This ID is used to access to multiple servers when running various scripts, copying data via RoboCopy, querying data across multiple databases across multiple servers and exporting data from External MS Applications – currently we use TEC accounts that have access rights across many servers. | Y | eDiscovery Manager | LRMT (28549) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_NOVARED3 |  |  | Account used by eDLS Team to access MS eDiscovery Compliance Center and Exchange Online  This ID is used to access to multiple servers when running various scripts, copying data via RoboCopy, querying data across multiple databases across multiple servers and exporting data from External MS Applications – currently we use TEC accounts that have access rights across many servers. | Y | eDiscovery Manager | LRMT (28549) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_NOVARED4 |  |  | Account used by eDLS Team to access MS eDiscovery Compliance Center and Exchange Online  This ID is used to access to multiple servers when running various scripts, copying data via RoboCopy, querying data across multiple databases across multiple servers and exporting data from External MS Applications – currently we use TEC accounts that have access rights across many servers. | Y | eDiscovery Manager | LRMT (28549) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_NOVARED5 |  |  | Account used by eDLS Team to access MS eDiscovery Compliance Center and Exchange Online  This ID is used to access to multiple servers when running various scripts, copying data via RoboCopy, querying data across multiple databases across multiple servers and exporting data from External MS Applications – currently we use TEC accounts that have access rights across many servers. | Y | eDiscovery Manager | LRMT (28549) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_NOVARED6 |  |  | Account used by eDLS Team to access MS eDiscovery Compliance Center and Exchange Online  This ID is used to access to multiple servers when running various scripts, copying data via RoboCopy, querying data across multiple databases across multiple servers and exporting data from External MS Applications – currently we use TEC accounts that have access rights across many servers. | Y | eDiscovery Manager | LRMT (28549) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_NOVARED7 |  |  | Account used by eDLS Team to access MS eDiscovery Compliance Center and Exchange Online  This ID is used to access to multiple servers when running various scripts, copying data via RoboCopy, querying data across multiple databases across multiple servers and exporting data from External MS Applications – currently we use TEC accounts that have access rights across many servers. | Y | eDiscovery Manager | LRMT (28549) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_NOVARED8 |  |  | Account used by eDLS Team to access MS eDiscovery Compliance Center and Exchange Online  This ID is used to access to multiple servers when running various scripts, copying data via RoboCopy, querying data across multiple databases across multiple servers and exporting data from External MS Applications – currently we use TEC accounts that have access rights across many servers. | Y | eDiscovery Manager | LRMT (28549) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_O365SVCACC01 |  |  | Global M365 Account. | Y | Company Administrator  TenantAdmins | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_O365SVCACC02 |  |  | Account used for Managing Tenant level activities. Also the account used for several automation solutions. | Y | Groups Administrator  Office Apps Administrator  Power BI Administrator  Power Platform Administrator  SharePoint Administrator  Teams Administrator  User Administrator  UserAccountAdmins | O365 SharePoint Online & OneDrive  (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_O365SVCACC03 |  |  | Account used for Managing Tenant level activities. Also the account used for several automation solutions. | Y | Groups Administrator  Office Apps Administrator  Power BI Administrator  Power Platform Administrator  SharePoint Administrator  Teams Administrator  User Administrator  UserAccountAdmins | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_O365SVCACC04 |  |  | Account used to manage the MS Teams administration with the devices. | Y | Teams Devices Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_O365SVCACC05 |  |  | Accounts used to login to dev, QA, Production servers. | N |  | O365 SharePoint Online & OneDrive (33371) | Account being reviewed for decommission | Can be revoked |
| TEC\_O365SVCACC06 |  |  | Accounts used to login to dev, QA, Production servers. | N |  | O365 SharePoint Online & OneDrive (33371) | Account being reviewed for decommission | Can be revoked |
| TEC\_O365SVCACC07 |  |  | Accounts used to login to dev, QA, Production servers. | N |  | O365 SharePoint Online & OneDrive (33371) | Account being reviewed for decommission | Can be revoked |
| ADM\_PPADMIN1 |  |  | Account used to login to dev, QA, production servers. Also this account is used by operations team to work on the operation activities. | Y | SharePoint Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be replaced with Tec account with similar role |
| ADM\_PPADMIN2 |  |  | Account used to login to dev, QA, production servers. Also this account is used by operations team to work on the operation activities. | Y | SharePoint Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be replaced with Tec account with similar role |
| ADM\_PPADMIN3 |  |  | Account used to login to dev, QA, production servers. Also this account is used by operations team to work on the operation activities. | Y | SharePoint Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be replaced with Tec account with similar role |
| ADM\_PPADMIN4 |  |  | Account used to login to dev, QA, production servers. Also this account is used by operations team to work on the operation activities. | Y | SharePoint Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be replaced with Tec account with similar role |
| ADM\_PPADMIN5 |  |  | Account used to login to dev, QA, production servers. Also this account is used by operations team to work on the operation activities. | Y | SharePoint Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be replaced with Tec account with similar role |
| ADM\_PPADMIN6 |  |  | Account used to login to dev, QA, production servers. Also this account is used by operations team to work on the operation activities. | Y | SharePoint Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be replaced with Tec account with similar role |
| ADM\_PPADMIN7 |  |  | Account used to login to dev, QA, production servers. Also this account is used by operations team to work on the operation activities. | Y | SharePoint Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be replaced with Tec account with similar role |
| ADM\_PPADMIN8 |  |  | Account used to login to dev, QA, production servers. Also this account is used by operations team to work on the operation activities. | Y | SharePoint Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be replaced with Tec account with similar role |
| ADM\_PPADMIN9 |  |  | Account used to login to dev, QA, production servers. Also this account is used by operations team to work on the operation activities. | Y | SharePoint Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be replaced with Tec account with similar role |
| TEC\_M365AdmAcc01 |  |  | Account used for managing and administrating PowerPlatform. | Y | Groups Administrator  Power Platform Administrator  SharePoint Administrator  Teams Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| TEC\_M365AdmAcc02 |  |  | Account used for managing and administrating PowerPlatform. | Y | Groups Administrator  Power Platform Administrator  SharePoint Administrator  Teams Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role. |
| SYS\_SPOAdmin1 |  |  | Account is used for managing and administrating the SharePoint/OneDrive services. Also it is used for User management activities e.g. Guest user off-boarding. | Y | O365 Super Administrator (Collective admin roles and lesser than Global Admin). | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *Acconts can be in application safe but required approved GAP* |
| ADM\_SPOADAD1 |  |  | Account is used for quering unified logs to run automation solutions. | Y | SharePoint Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be replaced with Tec account with similar role |
| ADM\_SPOADAD2 |  |  | Account is used for quering unified logs to run automation solutions. | Y | SharePoint Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be replaced with Tec account with similar role |
| ADM\_SPOADAD3 |  |  | Account is used for quering unified logs to run automation solutions. | Y | SharePoint Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be replaced with Tec account with similar role |
| ADM\_SPOADAD4 |  |  | Account is used for quering unified logs to run automation solutions. | Y | SharePoint Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *This account will be replaced with Tec account with similar role* |
| ADM\_SPOADAD5 |  |  | Account is used for quering unified logs to run automation solutions. | Y | SharePoint Administrator | O365 SharePoint Online & OneDrive (33371) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *This account will be replaced with Tec account with similar role* |
| TEC\_AIPADM01 |  |  | AIP owned account, used by AIP Team for performing AIP Admin activities like Label/Policy creation/updation, log collection, execution of Advanced setting command using powershell , script enhancements, debugging and testing scripts (if needed). | Y | Azure Information Protection administrator.  Sensitivity Label Administrator, Security Reader & View-Only Audit Logs in EXO | Azure Information Protection (44205) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | *This account will be retained as they have Azure AD role.* |
| TEC\_AIPADM02 |  |  | AIP owned account which is currently performing AIP encryption for OCD Carbon solution. Currently the page transition is ongoing for carbon OCD and this account will be used and owned by AIP team only, as Carbon OCD solution will be transitioned to page AES team, and they will be using separate account. | Y | Azure Information Protection administrator &  Sensitivity Label Administrator | Azure Information Protection  (44205) | *Cannot be handed over to PAGE due to high risk Platform level permissions* | This account will be retained as they have Azure AD role |
| TEC\_AIPDEV |  |  | On AIP Database server,this account is used for Scheduled Task called ‘Run AIP GMT Import’ – which runs the PowerShell script called AIPGMT.ps1.Script adds the license user automatically to GMT groups scoped under Global policy. Going forward, it may also be used in ADP (Automatic Decryption Process). | N |  | Azure Information Protection  (44205) | Mukesh had informed that it should not be transitioned to PAGE as we will have dependency on PAGE Team for testing / troubleshooting purpose as we will have to raise request with them for this so that they can do screenshare session. This is because safe of account will be owned by them if we decide to transition this account. | *This account will be retained as they have Azure AD role.* |
| TEC\_AIPSU01 |  |  | Super User role is assigned to this account. Used by AIP Team for performing decryption activities of files and PST.Currently,this account is being used for Automatic Decryption Process (ADP). | N |  | Azure Information Protection  (44205) | Cannot be handed over to PAGE due to high risk Platform level permissions which can unecrypt any data and scoped under Platform use. | This account can be retained. |
| TEC\_AIPSU02 |  |  | Super User role is assigned to this account. Used by AIP Team for performing decryption activities of files and PST. Going forward, it may also be used in ADP (Automatic Decryption Process). | N |  | Azure Information Protection  (44205) | Cannot be handed over to PAGE due to high risk Platform level permissions which can unecrypt any data and scoped under Platform use. | This account can be retained. |
| TEC\_AIPLOG1 |  |  | This account is used in the script running on server GLCHBS-SP321007 for collecting AIP logs.Also, used to take RDP, scheduled task execution and troubleshooting script issues. | N |  | Azure Information Protection  (44205) | This account can’t be transitioned to PAGE Team as we will have dependency on them for raising request and screen sharing for any troubleshooting / debugging purpose. This is because the safe of account will be transitioned to them and we will not be able to see it in PAM. | Scheduled task can be operated through sys accounts hence this can be replaced with sys accounts. |
| SYS\_AIPLOSY1 |  |  | Used to logon to AIP Service and get / download user logs on server, GLCHBS-SP321007 which is later forwarded to Splunk. | Y | Azure Information Protection Administrator role | Azure Information Protection  (44205) | This account cannot be transferred to PAGE Team as it has cloud role assigned. | This account can be retained. |
| SYS\_AIPLOG1 |  |  | Alias in PAM is eunet/sys\_aiplog1 and username is sys\_aiplosy1, hence this is same account as SYS\_AIPLOSY1. Used to logon to AIP Service and get / download user logs on server, GLCHBS-SP321007 which is later forwarded to Splunk. | Y | Azure Information Protection Administrator role | Azure Information Protection  (44205) | This account cannot be transferred to PAGE Team as it has cloud role assigned. | This account can be retained |
| SYS\_AIPSU1 |  |  | Super User role was assigned to this account. It was used by AIP Team for performing decryption activities of files and PST. | N |  | Azure Information Protection  (44205) | This is our old super user account which is not in use now | Can be revoked |
| SYS\_AIPSU2 |  |  | Super User role was assigned to this account. It was used by AIP Team for performing decryption activities of files and PST. | N |  | Azure Information Protection  (44205) | This is our old super user account which is not in use now | Can be revoked |
| ADM\_NBNRA1 |  |  | ADM account of Ramesh NBN. | N |  | Azure Information Protection  (44205) | This is not a privileged account and should not be transferred to PAGE Team in transition. Access from server, GLCHBS-SP320603 can be removed. | Replace with App domain account. |
| DHUSIGA1 |  |  |  | N |  | Azure Information Protection  (44205) | This is not a privileged account and should not be transferred to PAGE Team in transition. This account belongs to Gaurav Dhusia. Access from server, GLCHBS-SP320603 can be removed. | Personal accounts are not allowded and will be revoked. |
| PATOUMO1 |  |  |  | N |  | Azure Information Protection  (44205) | This is not a privileged account and should not be transferred to PAGE Team in transition. Access from server, GLCHBS-SP320603 can be removed. | Personal accounts are not allowded and will be revoked. |
| APP01 |  |  | Local account for production server, GLCHBS-SP320603, GLCHBS-SP320791, GLCHBS-SP360211, FANET / PPE server, GLCHBS-SP320820 and server, GLCHBS-ST320491 (this server is showing as retired in SNOW) | N |  | Azure Information Protection  (44205) | Since they are not privileged account as per PAGE Team, it’s not subjected to transition. | Can be revoked |
| APP02 |  |  | Local account for production server, GLCHBS-SP320603, GLCHBS-SP320791, GLCHBS-SP360211, FANET / PPE server, GLCHBS-SP320820 and server, GLCHBS-ST320491 (this server is showing as retired in SNOW) | N |  | Azure Information Protection  (44205) | Since they are not privileged account as per PAGE Team, it’s not subjected to transition. | Can be revoked. |
| TSP\_TO365T3G |  |  | FANET account, which was used to login to pre-production server, GLCHBS-SP320820 to perform super user activities and production server, GLCHBS-SP320603 | N |  | Azure Information Protection  (44205) | Since FANET / PPE domain is already decommissioned, no action is required for this account. | Can be revoked. |
| TEC\_0365LSA2 |  |  | Used to login to Teams powershell and Teams admin center. | Y | Reports Reader;  Service Support Administrator;  Skype for Business Administrator;  Teams Administrator;  Teams Communications Administrator;  Teams Communications Support Engineer;  Team Communications Support Specialist;  ServiceSupportAdmins | Microsoft Teams (44104) | Cannot be handed over to PAGE due to high risk Platform level permissions. | This account can be retained. |
| TEC\_MESSASU2  TEC\_MESSASU3  TEC\_MESSASU4  TEC\_MESSASU5  TEC\_MESSASU6  TEC\_MESSASU7  TEC\_MESSASU8  TEC\_MESSASU9 |  |  | Accounts used by Messaging L2 operations team | N |  | Exchange Messaging (31727) | This requires review with the technical team if the ownership could be handed over and replace with App / JIT accounts. | This account can be retained. |
| TEC\_COREMOP1  TEC\_COREMOP2 |  |  | Accounts used by Messaging L4 operations team | Y | Exchange Online (Organization Configuration) | Exchange Messaging (31727) | Cannot be handed over to PAGE due to high risk Platform level permissions. | This account can be retained. |
| TEC\_COREMOP4  TEC\_COREMOP5  TEC\_COREMOP6  TEC\_COREMOP7  TEC\_COREMOP8 |  |  | Accounts used by Messaging L4 operations team and M&A | Y | Exchange Online  License Administrator | Exchange Messaging (31727) | Cannot be handed over to PAGE due to high risk Platform level permissions. | This account can be retained. |
| TEC\_COREMCS3  TEC\_COREMCS4  TEC\_COREMIS2  TEC\_COREMVI1 |  |  | Account used by Corporate Security, ISRM and VIP Support | N |  | Exchange Messaging (31727) | To be discussed with ISRM. | This account can be retained. |

## Access to SYS\_accounts in PAM

# Prerequisites

| **Definition** | **Description** |
| --- | --- |
|  |  |
|  |

# Risks and challenges

| **Definition** | **Mitigation** |
| --- | --- |
|  |  |

# References, Attachments, Abbreviations/Acronyms

## References

| **#** | **ID** | **Title** |
| --- | --- | --- |
|  | ISRM\_IAM\_PAGE\_PC\_001 | PAGE Project Charter |

## Attachments

| **#** | **ID** | **Title** |
| --- | --- | --- |
|  | Account Type Definitions V4.1.xlsx | New account type definitions |
|  | PAGE Overview 2020-01.pptx | PAGE principles overview |

## Abbreviations / Acronyms

| **Terminology** | **Description** |
| --- | --- |
| DEC | Decision Document |