# THESIS – CYBERSECURITY COURSE 2021/2022

Office365 systems: Teams Information Barriers

proposed by @Avanade

**MARIO CUOMO**

# Summary

# ABSTRACT

3 are the main goals of cybersecurity: to ensure the confidentiality, integrity, and availability of data. Among the various tools made available by Microsoft to ensure confidentiality there is Information Barriers, a tool from Microsoft 365 – a set of tools for productivity, business management, security, and compliance. Computer systems acquire a huge amount of data and attention to these is fundamental. In the context of business productivity, data means any resource useful to carry out its activities; very often these resources are shared in collaboration tools, such as *Microsoft Teams*.

The purpose of *Information Barriers* is to make sure that the resources are shared only among those with access rights limiting their dissemination – even within the same organization. The implementation of *information barriers* can be carried out both for legislative reasons – for example compliance with directives such as the GDPR of 2018 – but also for internal company policies – for example by limiting the possibility of communication between two departments such as administration and commercial.

*Information Barriers* helps to protect information within organizations by focusing on compliance rather than identity and security, defining who is or is not allowed to share content with whom.

Although you can apply *Information Barriers* to different tools, such as *SharePoint* and *OneDrive*, the following paper has the focus for *Microsoft Teams* platform.

## REQUIREMENTS

To use *Information Barriers* you must have one of the following licenses:

- Microsoft 365 E5/A5
- Office 365 E5/A5/A3/A1
- Microsoft 365 E3/A3/A1 + Microsoft 365 E5/A5 Compliance
- Microsoft 365 E3/A3/A1 + Microsoft 365 E5/A5 Insider Risk Management

For the sole purpose of testing, you can activate the Office 365 E5 license for free for one month by visiting the following web page:
*https://signup.microsoft.com/get-started/signup?products=101bde18-5ffb-4d79-a47b-f5b2c62525b3*
The tenant I created is @cybermario.onmicrosoft.com.

Microsoft E5 trial offers the possibility of creating maximum 25 users –enough to test the different policies described in the paper.

The possession of the license is a necessary but not sufficient condition.
The person who will create and manage the information barrier policies must have one of the following roles:

- Microsoft 365 Global Administrator
- Office 365 global admin
- Compliance Administrator
- IB Compliance Management

Once the trial is activated, an Office global administrator user is automatically created with the data of the user to whom the trial is associated. The global administrator can add new users: you can do this through the 365 *https://admin.microsoft.com/Adminportal* admin center or through *PowerShell*. It is important to note that all affected users have an Office license 365.

```
Connect-MsolService

New-MsolUser -DisplayName "Alessandro Rossi" -FirstName Alessandro -LastName Rossi -
UserPrincipalName alessandrorossi@cybermario.onmicrosoft.com -UsageLocation IT -
LicenseAssignment cybermario:ENTERPRISEPREMIUM
```

Before implementing policies for *Information Barriers,* you need to be sure that *Audit Logging* is enabled in Office365. *Audit logging* is one of the phases of the *AAA* model: *Authentication, Authorization* and *Accountability.*
When we talk about the *AAA* model in cybersecurity, the third *A* has a double meaning: *Accountability* or *Auditing.* When we refer to *Auditing,* we want to check if the system conforms to what we have previously established; when we refer to *Accountability,* we want to make sure that it is possible to associate an event or action with one or more responsible parties.
*Audit Logging* is the component in Office 365 that performs both roles.

The activation of *Audit* Logging takes place *either* through the web portal – *compliance.microsoft.com/auditlogsearch* – or through *PowerShell*

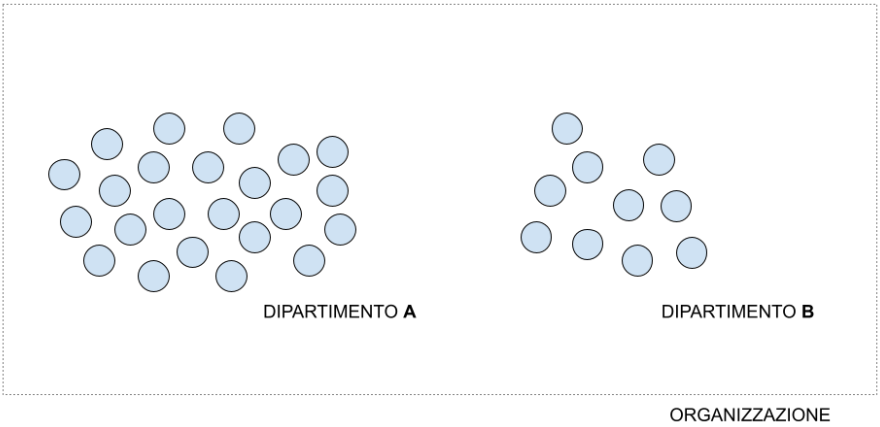
```
Import-Module ExchangeOnlineManagement


Connect-ExchangeOnline -UserPrincipalName mariocuomo@cybermario.onmicrosoft.com

Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true
```

Finally, to use *Information Barriers* in *Microsoft Teams* is to enable directory-scope search by using an Exchange address book *policy.* This feature is easily activated in the *Teams* admin portal at the following address *https://admin.teams.microsoft.com/company-wide-settings/teams-settings*

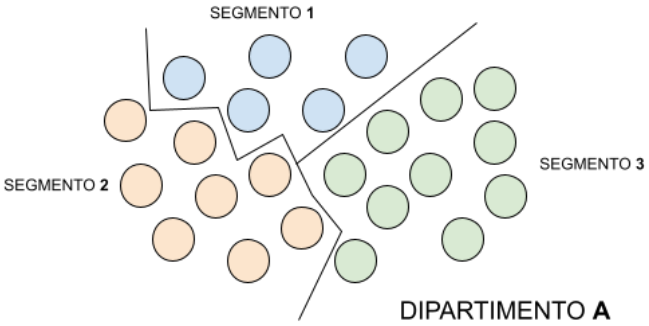
## HIGH-LEVEL OVERVIEW

One of the main concepts when working with *Information Barriers* is that of *segment*.
A segment uniquely identifies a group of users.
Identifying segments is a non-trivial operation: a user can belong to one and only one segment, and only one criterion can be applied to each of them.

In the simplest cases a segment can be identified starting from an intrinsic characteristic of users such as belonging to one department rather than another.
The properties that can be used are all those used in *Azure Active Directory,* an identity management service on the *Microsoft cloud*.




A more complex operation occurs if you want to make a segmentation to a finergrain, for example by segmenting users belonging to the same department and not having a discriminating feature for them. In this case it is possible to define custom properties.




Once the segments have been identified and defined, it is necessary to establish the criterion to limit communication between them.
Note how *policies* are bidirectional: if you want to block communication between the segment 1 and the segment 2 you need to define two criteria for both communication flows from one segment to another.

In general, the definition and activation of policies takes place at two distinct temporal moments, often after a careful review of the defined criteria, as the activation of these is not immediate but takes a handful of hours.

## BUSINESS SCENARIO

As a sample business scenario for use cases 1and 2 I considered the Tenant Office 365 of Roma Tre University.

Doing a user search using Microsoft Teams I noticed that you can start a new conversation with any category of person who owns an Office 365 user of the tenant of university *@[xxx]. uniroma3.it*.
For example, secretarial staff can start a conversation with a professor at any time. The same can happen between administration staff and students.

Sometimes you want to avoid this situation because it is possible that unauthorized users come into possession of sensitive data shared incorrectly within the Microsoft Teams platform. Think, for example, of an administrator who wants to share a file on Teams to another administrator but mistakes the user – sending it to a student – because of a homonymy.

For simplicity consider the organization formed as follows:

| DEPARTMENT |
|---|
| ENGINEERING |
| LITERATURE |
| ADMINISTRATION |
| FRONTOFFICE |
| TREASURY |

In an even more simplistic way, consider to have the only information as the *name, surname* and *department*.

| NAME | SURNAME | DEPARTMENT |
|---|---|---|
| MARIO | ROSSI | ENGINEERING |
| LUCA | VERDI | LITERATURE |
| … | … | … |

At present, every user in each department can start a new conversation with any other user.
In the use case 1 it is shown how to block communication between segments: students of *Engineering* and *Literature* will not be able to interact with the staff of the *Administration.*
In the use case 2 it is shown how to isolate communication to and from the outside of a segment: treasury staff can share data only between the group itself.

## CONNECTION TO SECURITY & COMPLIANCE CENTER

The application of *Information Barriers* is mainly done via scripting through *PowerShell,* a command shell that uses the scripting language of the same name based on the *.NET Common Language Runtime.*
In preview you can also work with *Information Barriers* through the user interface in the *https://compliance.microsoft.com* administration panel.

The first step is to give consent to the *Infomation Barrier Processor* to access the information of the application and tenant of interest by connecting to the tenant on *Azure.*

```
Connect-AzureAD -Tenant cybermario.onmicrosoft.com

$appId="bcf62038-e005-436d-b970-2a472f8c1982"

$sp=Get-AzureADServicePrincipal -Filter "appid eq '$($appid)'"

if ($sp -eq $null) { New-AzureADServicePrincipal -AppId $appId }

Start-Process
"https://login.microsoftonline.com/common/adminconsent?client_id=$appId"
```

Once provided consent you access the *Security & Compliance Center* as follows:

```
Connect-IPPSSession -UserPrincipalName mariocuomo@cybermario.onmicrosoft.com
```

From this moment it is possible to define segments and policies.
The use cases described below do not report the connection and authentication phase, a preliminary operation in any case.

## USE CASE 1 – BLOCK COMMUNICATION TO A SPECIFIC INTERNAL GROUP

The policy that you want to implement in this case is very simple: students belonging to the departments of *Engineering* and *Literature* cannot share information with the staff of *Administration.* Similarly, the *Administration* cannot start a conversation with the two departments.
Think of a policy where you need to contact the front office as a proxy between the two entities.

The first step is to define 3 user segments.
Segmentation occurs based on the *Department* property associated with each user.

```
New-OrganizationSegment -Name "Engineering" -UserGroupFilter "Department -eq
'Engineering'"

New-OrganizationSegment -Name "Literature" -UserGroupFilter "Department -eq
'Literature'"

New-OrganizationSegment -Name "Administration" -UserGroupFilter "Department -eq
'Administration'"
```

Once the requirements have been defined, the criteria to be implemented are defined.
Policies can be mainly of 2 different categories: *blocking policies* that prevent communication between segments, *allow* type policies that allow communication only to specified segments.

A block policy will be used in this use case.

```
New-InformationBarrierPolicy -Name "Engineering-Administration" -AssignedSegment
"Engineering" -SegmentsBlocked "Administration" -State Inactive
```

The command described above creates a policy named *Engineering-Administration* assigned to the segmentor *Engineering*, is of a blocking type against the *Administration* segment.
The policy is inactive: it still has no effect on users.

The newly made block is *one-way,* it blocks communication from any account of the *Engineering* department to any account of the *Administration* department.
To make a bidirectional block you need to define a second criterion, like the previous one.

```
New-InformationBarrierPolicy -Name " Administration-Engineering " -AssignedSegment "
Administration " -SegmentsBlocked "Engineering" -State Inactive
```

As has been done for the Department of *Engineering,* other 2 criteria must be created for blocking information regarding communication from *Administration* to *Literature* and vice versa (called *Administration-Literature* and *Literature-Administration* respectively).

In a more elegant and clean way it is possible to achieve everything with 3 policies by combining in a single criterion the block of communication that starts from the users of the *Administration.*
The official documentation – docs.microsoft.com/it-it/microsoft-365/compliance/information-barriers-policies – suggests not to assign more than one criterion to each segment to improve the analysis and be more easily compliant with internal and external regulations of the organization.

```
New-InformationBarrierPolicy -Name "Administration-LiteratureEngineering" -
AssignedSegment "Administration" -SegmentsBlocked "Engineering","Literature" -State
Inactive
```

The general situation is as follows

| ADA | ENGINEERING | LITERATURE | ADMINISTRATION | FRONTOFFICE | TREASURY |
|---|---|---|---|---|---|
| ENGINEERING | ✓ | ✗ | ✗ | ✓ | ✓ |
| LITERATURE | ✓ | ✓ | ✗ | ✓ | ✓ |
| ADMINISTRATION | ✗ | ✗ | ✓ | ✓ | ✓ |
| FRONTOFFICE | ✓ | ✓ | ✓ | ✓ | ✓ |
| TREASURY | ✓ | ✓ | ✓ | ✓ | ✓ |

The activation of the policies takes place explicitly after the creation of these, even after some time.

To check the current state of all defined policies you can use the following command

```
Get-InformationBarrierPolicy
```

Each policy is characterized by a *name* – specified during creation – and a *GUID* – assigned by the system.
To make a policy in active mode, you must do:

```
Set-InformationBarrierPolicy -Identity "Administration-LiteratureEngineering" -State
Active
```

To start applying policies to users you must run:

```
Start-InformationBarrierPoliciesApplication
```

The policy will be applied for each user of the segments involved: it follows that if the organization is very large, the activation process can take a time even of the order of a day.
Conversely, you can block the process of activating a policy quickly – estimated half an hour.

```
Stop-InformationBarrierPoliciesApplication -Identity <GUID>
```

## USE CASE 2 – ISOLATION OF USERS OF A GROUP

In the use case 2 you want to implement a blocking policy from one segment to all the others.
The segment that is considered is that of the *Treasury* department: monetary sensitive data should remain well confined and not disclosed to unauthorized persons.
*Treasury* users will only be able to communicate with each other.

First you create a segment, as seen in the use case 1

```
New-OrganizationSegment -Name "Treasury" -UserGroupFilter "Department -eq 'Treasury'"
```

To achieve the isolation of users in the segment from all other users can be done in two ways. The first is to create $n - 1$ policies (if $n$ is the numbers of segments identified): this strategy is very time-consuming and goes against the principle that only one criterion must be applied to each segment. Finding a new segment changes the criteria that have already been defined.
The second way to achieve an isolation of this kind is the use of a policy of type *consent:* when you make such a policy you declare only the segments with which communication is allowed (which in this case there are none, if not the segment itself).

```
New-InformationBarrierPolicy -Name "Treasury-to-Treasury" -AssignedSegment "Treasury"
-SegmentsAllowed "Treasury" -State Inactive
```

Unfortunately, this policy alone does not work.
*Information Barriers* need 2 pathway policies. With the previous command, communication from the *Treasury* segment to all the others has been blocked: it is necessary to block communication from all other segments to the treasury.
6 policies are created: 5 policies blocking from the segments *Engineering, Literature, Administration, FrontOffice* to *Treasury* and 1 *blocking* communication from Treasury to others (which can be realized as seen in the precedence or creating a blocking policy as follows).

```
New-InformationBarrierPolicy -Name "Treasury-to-Treasury" -AssignedSegment "Treasury"
-SegmentsBlocked "Engineering","Literature","Administration","FrontOffice" -State
Inactive
```

The general situation is as follows

| TO / FROM | ENGINEERING | LITERATURE | ADMINISTRATION | FRONTOFFICE | TREASURY |
|---|---|---|---|---|---|
| ENGINEERING | ✓ | ✓ | ✓ | ✓ | ✗ |
| LITERATURE | ✓ | ✓ | ✓ | ✓ | ✗ |
| ADMINISTRATION | ✓ | ✓ | ✓ | ✓ | ✗ |
| FRONTOFFICE | ✓ | ✓ | ✓ | ✓ | ✗ |
| TREASURY | ✗ | ✗ | ✗ | ✗ | ✓ |

The same precautions apply as seen for the case 1 regarding the activation of the policy and the expected timing.

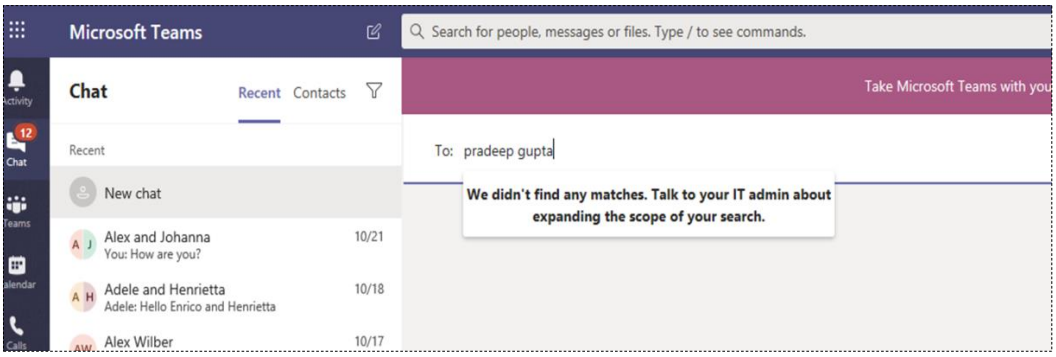
## EFFECTS IN THE APPLICATION OF INFORMATION BARRIERS

It has been seen how to block sharing and communication between segments, but it has not been explicitly specified what this entails.
Among the effects of *Information Barriers* on the various *SharePoint Online* and *OneDrive for Business* tools, the focus of this paper is on the *Microsoft Teams* platform.

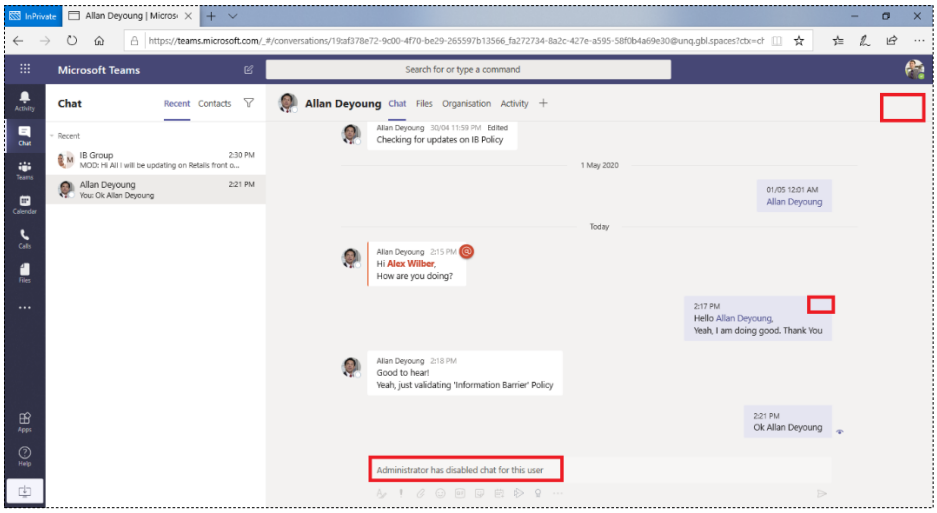
Considering a blocking policy between segment *A* and segment *B,* and simple blocks that can occur as follows:

- A user $a$ in segment *A* wants to start a conversation with a user $b$ in segment *B.*
  When the user $a$ searches for the user's name $b$ in *Microsoft Teams,* that user is not found.
  You are not explicitly warned about information *barriers,* but you are encouraged to contact your administrator to try expanding your search domain.

  The same happens when $a$ try to add $b$ to a team.




- If no criteria were previously defined between segments, it is likely that a user $a$ in segment *A* has previously communicated with a user $b$ in segment *B.*
  From the moment you enable the policy, chat (messages, calls, video calls, and screen sharing) between the two is disabled.



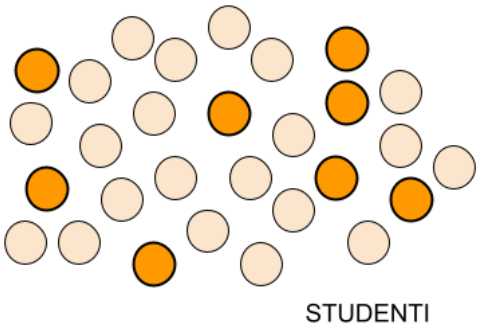
## USE CASE 3 – SEGMENTING USERS USING CUSTOM FEATURES

One of the biggest complexities working with information barriers is the constraint that a user can belong to at most one segment.
More than a constraint is a strong recommendation: imagine the situation in which a user belongs to two different segments (segment *A* and segment *B)*. The segments in question have two policies contrasts towards a third segment *C: A* can communicate with C, *B* cannot communicate with *C*. Since the policy for the user is not univocally defined, there could be an abnormal behavior in communication.

Where it is not possible to comply with the constraint of segmentation using the intrinsic characteristics of the user – geographical location, department, etc. – it is possible to resort to the application of ad hoc custom features.

The use case 3 considers the following scenario: you want to group an elite of *Engineering* and *Literature* students for a private project. They want to keep existing users with the policy that elite users are isolated from the other students.
You can segment users using one of the 14 custom attributes made available for each user in *Azure Active Directive.*
You can use PowerShell as follows to add *extensive attributes.*

```
Connect-ExchangeOnline -UserPrincipalName mariocuomo@cybermario.onmicrosoft.com

Set-Mailbox -Identity mariocuomo@cybermario.onmicrosoft.com -CustomAttribute1 Elite
```



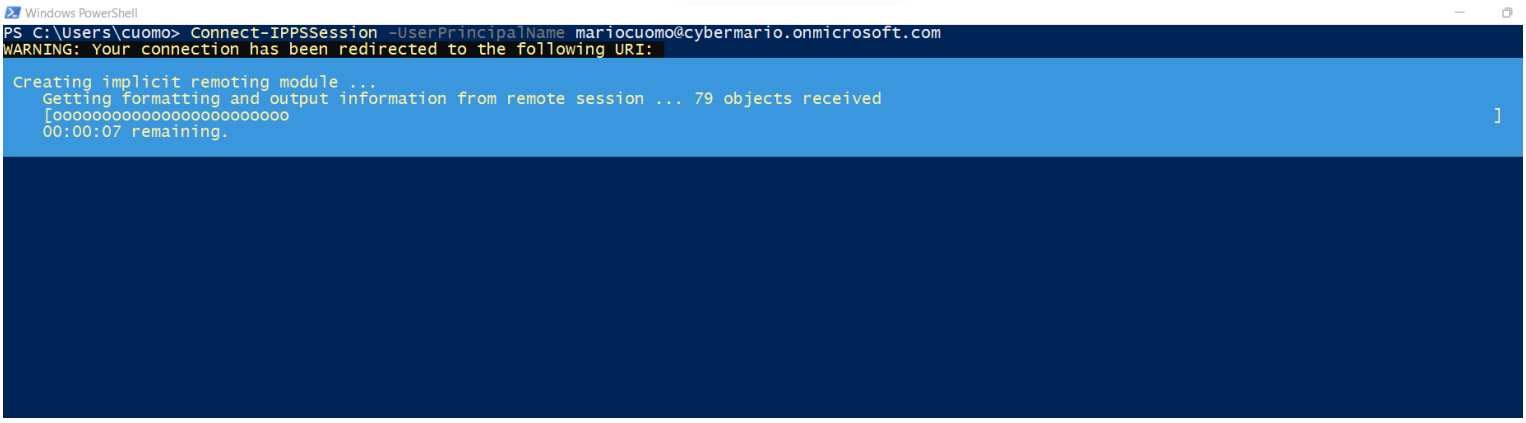

At this point you can create the segments using the new feature as a discriminating agent and then you can set the *barrier policies* – in the specific case of type *allowed* that allow only communication between internal members and not towards external ones (as seen for the use case 2).

# SCREENSHOTS AND USEFUL COMMANDS

## Connect-IPPSSession

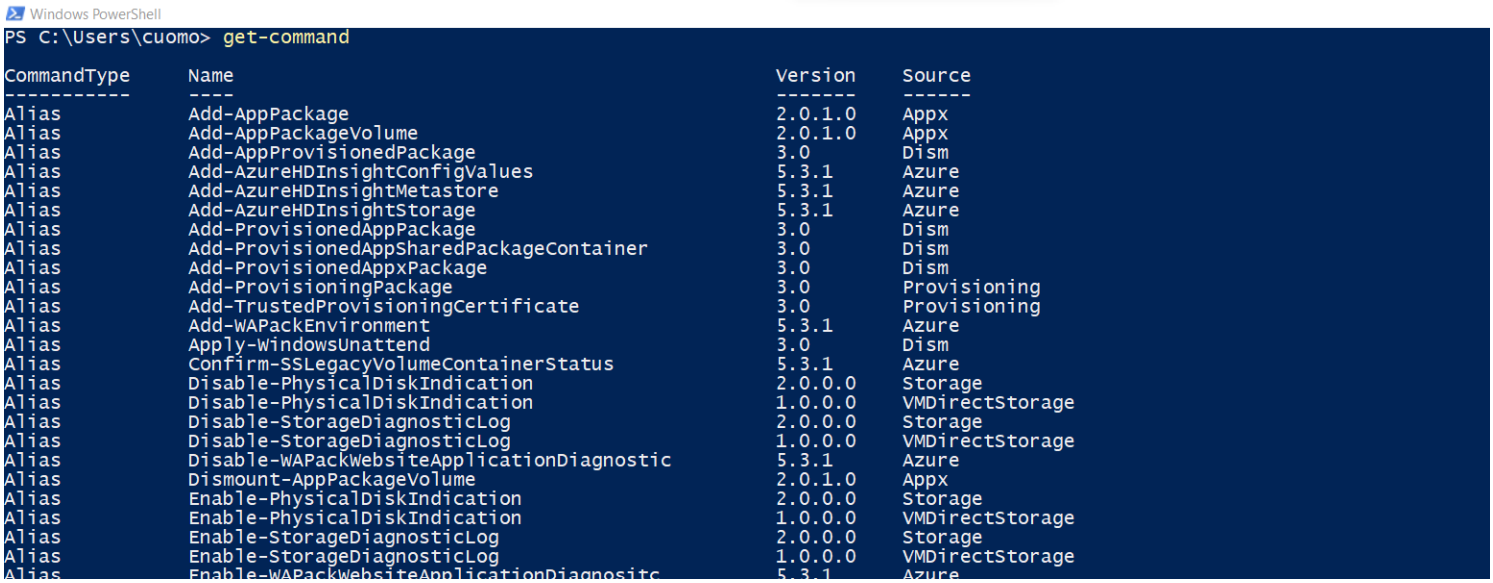
With this command, you can connect to the *Security and Compliance Center* and manage *Information Barriers.*

```
Connect-IPPSSession -UserPrincipalName mariocuomo@cybermario.onmicrosoft.com
```




During the connection, all commands to create segments and policies are enabled.
To check the available commands, you can run the following command:

```
get-command
```




If you do not find the required cmdlets, import the *Exchange Online* module and connect again.

```
Import-Module ExchangeOnlineManagement
```

If you still do not find the cmdlets, check the requirements again.
Cmdlets are enabled when you import the required modules and have permissions to run them.

## New-OrganizationSegment

With this command you can create new segments.
It is a logical partition of users based on a common feature.
To create a segment named *Biologia* that consists of all users who belong to the *Biologia* department, run the following command:

```
New-OrganizationSegment -Name "Biologia" -UserGroupFilter "Department -eq 'Biologia'"
```

```
Select Windows PowerShell
PS C:\Users\cuomo> New-OrganizationSegment -Name "Biologia" -UserGroupFilter "Department -eq 'Biologia'"


RunspaceId             : 3ad38d4c-589c-41d8-939c-44b644d9313c
Type                   : OrganizationSegment
UserGroupFilter        : Department -eq 'Biologia'
ExoSegmentId           : fd43d5ba-8fbe-4709-ac4d-dbbc91e09421
ObjectVersion          : 18b0b454-fd74-4da9-a6d6-08d9d43ad3f7
CreatedBy              : Mario Cuomo
LastModifiedBy         : Mario Cuomo
Comment                :
ModificationTimeUtc    : 10/01/2022 13:12:17
CreationTimeUtc        : 10/01/2022 13:12:17
Identity               : FFO.extest.microsoft.com/Microsoft Exchange Hosted Organizations/cybermario.onmicrosoft.com/Configuration/Biologia
Id                     : FFO.extest.microsoft.com/Microsoft Exchange Hosted Organizations/cybermario.onmicrosoft.com/Configuration/Biologia
ExchangeVersion        : 0.20 (15.0.0.0)
Name                   : Biologia
DistinguishedName      : CN=Biologia,CN=Configuration,CN=cybermario.onmicrosoft.com,OU=Microsoft Exchange Hosted
                         Organizations,DC=FFO,DC=extest,DC=microsoft,DC=com
ObjectCategory         :
ObjectClass            : {msExchUnifiedPolicy}
WhenChanged            : 10/01/2022 14:12:17
WhenCreated            : 10/01/2022 14:12:17
WhenChangedUTC         : 10/01/2022 13:12:17
WhenCreatedUTC         : 10/01/2022 13:12:17
ExchangeObjectId       : 761cf3a8-1b5b-4c8e-a1dd-a4d9078e535c
OrganizationalUnitRoot : FFO.extest.microsoft.com/Microsoft Exchange Hosted Organizations/cybermario.onmicrosoft.com
OrganizationId         : FFO.extest.microsoft.com/Microsoft Exchange Hosted Organizations/cybermario.onmicrosoft.com - FFO.extest.microsoft.com/Microsoft
                         Exchange Hosted Organizations/cybermario.onmicrosoft.com/Configuration
Guid                   : 761cf3a8-1b5b-4c8e-a1dd-a4d9078e535c
OriginatingServer      :
IsValid                : True
ObjectState            : New
```

Notice how you can define expressions that are complex enough to identify segments.

```
New-OrganizationSegment -Name "HRIndeterminato" -UserGroupFilter " Department -eq
'HR' -and Position -ne 'Indeterminato'"
```

It is returned in output a *.NET* object that presents several useful information such as the user who created it and the last modification made.
The *Guid* and the *DistinguishedName* are very important information used to uniquely identify an *OrganizationSegment.*

## New-InformationBarrierPolicy

With this command you can define a policy between segments.
Policies can be *blocked* by defining the segments to which communication is blocked or *allowed* by defining the segments to which communication is allowed.
To create a policy that blocks communication from the *Segreteria* segment to the *Tesoreria* segment, run the following command:

```
New-InformationBarrierPolicy -Name "Segreteria-Tesoreria" -AssignedSegment
"Segreteria" -SegmentsBlocked "Tesoreria" -State Inactive
```

```
Windows PowerShell
PS C:\Users\cuomo> New-InformationBarrierPolicy -Name "Segreteria-Tesoreria" -AssignedSegment "Segreteria" -SegmentsBlocked "Tesoreria" -State Inactive

Note: Information barrier policy will restrict communication, collaboration and people search between users.

For Teams  - including Teams Channel (Microsoft 365 Groups), Teams Meeting & Teams Communication (Chat, Call)
 * Access to communication/content access/people search/SharePoint site
   connected to the Teams will be restricted based on Information Barrier
   policy assigned to user's segments.

For OneDrive
 * Access and sharing of OneDrive content will be restricted based on the
   information barrier policy assigned to the OneDrive owner.

For SharePoint- including Microsoft 365 Groups connected and non-connected sites
 * Segments are associated to a SharePoint site (communication sites,
   classic sites, modern sites) based on the site creator's segment or by
   adding segments explicitly to a site.
 * Access and sharing of a SharePoint site will be restricted to the
   segments associated to the site.
   More Details - https://aka.ms/SPOInfobarriers.

Are You Sure You Want To Proceed?
[Y] Yes  [N] No  [?] Help (default is "Y"): Y


RunspaceId              : 3ad38d4c-589c-41d8-939c-44b644d9313c
Type                    : InformationBarrier
AssignedSegment         : Segreteria
SegmentsAllowed         : {}
ExoPolicyId             : c6bf3a5d-4980-43f8-b187-f12b2b6cb2fb
SegmentsBlocked         : {Tesoreria}
SegmentAllowedFilter    :
BlockVisibility         : True
BlockCommunication      : True
State                   : Inactive
ObjectVersion           : 91f67d44-7b52-4f9c-84a9-08d9d4409fef
CreatedBy               : Mario Cuomo
LastModifiedBy          : Mario Cuomo
Comment                 :
ModificationTimeUtc     : 10/01/2022 13:53:47
CreationTimeUtc         : 10/01/2022 13:53:47
Identity                : FFO.extest.microsoft.com/Microsoft Exchange Hosted Organizations/cybermario.onmicrosoft.com/Configuration/Segreteria-Tesoreria
Id                      : FFO.extest.microsoft.com/Microsoft Exchange Hosted Organizations/cybermario.onmicrosoft.com/Configuration/Segreteria-Tesoreria
ExchangeVersion         : 0.20 (15.0.0.0)
Name                    : Segreteria-Tesoreria
DistinguishedName       : CN=Segreteria-Tesoreria,CN=Configuration,CN=cybermario.onmicrosoft.com,OU=Microsoft Exchange Hosted
                          Organizations,DC=FFO,DC=extest,DC=microsoft,DC=com
ObjectCategory          :
ObjectClass             : {msExchUnifiedPolicy}
WhenChanged             : 10/01/2022 14:53:47
WhenCreated             : 04/01/2022 14:47:20
WhenChangedUTC          : 10/01/2022 13:53:47
WhenCreatedUTC          : 04/01/2022 13:47:20
ExchangeObjectId        : 50ef5287-611f-4d47-ae20-3f8398110183
OrganizationalUnitRoot  : FFO.extest.microsoft.com/Microsoft Exchange Hosted Organizations/cybermario.onmicrosoft.com
OrganizationId          : FFO.extest.microsoft.com/Microsoft Exchange Hosted Organizations/cybermario.onmicrosoft.com - FFO.extest.microsoft.com/Microsoft
                          Exchange Hosted Organizations/cybermario.onmicrosoft.com/Configuration
Guid                    : 50ef5287-611f-4d47-ae20-3f8398110183
OriginatingServer       :
IsValid                 : True
ObjectState             : Unchanged
```

It is returned in output a *.NET* object that presents various useful information such as the user who created the policy, which segment it is associated with and which are the segments to which communication is blocked/allowed.
The *Guid* and *DistinguishedName* are very important information used to uniquely identify a policy.
The *state* is a property that indicates whether the policy is active or not.

Note how the policies must be bidirectional: if you block communication from *Segreteria* to *Tesoreria* you must also block communication from *Tesoreria* to *Segreteria.*
You can create *InformationBarrierPolicy* that are not bidirectional without raising exceptions. The exception is raised when trying to activate them.

## Set-InformationBarrierPolicy & Get-InformationBarrierPolicy

With the first command you can change the properties of a policy.
The greatest use is that of the change of *state:* from *Active* to *Inactive* and vice versa.

You can add an explanatory comment to a policy with the following command:

```
Set-InformationBarrierPolicy -Identity "Segreteria-Tesoreria" -Comment "Block
communication from Segreteria to Tesoreria"
```

To get information about a specific policy, use the second command as follows:

```
Get-InformationBarrierPolicy -Identity "Segreteria-Tesoreria"
```

```
Windows PowerShell
PS C:\Users\cuomo> Set-InformationBarrierPolicy -Identity "Segreteria-Tesoreria" -Comment "Blocca la comunicazione da Segreteria a Tesoreria"

Note: Information barrier policy will restrict communication, collaboration and people search between users.

For Teams  - including Teams Channel (Microsoft 365 Groups), Teams Meeting & Teams Communication (Chat, Call)
 * Access to communication/content access/people search/SharePoint site
   connected to the Teams will be restricted based on Information Barrier
   policy assigned to user's segments.

For OneDrive
 * Access and sharing of OneDrive content will be restricted based on the
   information barrier policy assigned to the OneDrive owner.

For SharePoint- including Microsoft 365 Groups connected and non-connected sites
 * Segments are associated to a SharePoint site (communication sites,
   classic sites, modern sites) based on the site creator's segment or by
   adding segments explicitly to a site.
 * Access and sharing of a SharePoint site will be restricted to the
   segments associated to the site.
   More Details - https://aka.ms/SPOInfobarriers.

Are You Sure You Want To Proceed?
[Y] Yes  [N] No  [?] Help (default is "Y"):
WARNING: Your changes will take into affect after you run Start-InformationBarrierPoliciesApplication cmdlet. Start-InformationBarrierPoliciesApplication cmdlet only
applies Active state policies.
PS C:\Users\cuomo> Get-InformationBarrierPolicy -Identity "Segreteria-Tesoreria"


RunspaceId              : 3ad38d4c-589c-41d8-939c-44b644d9313c
Type                    : InformationBarrier
AssignedSegment         : Segreteria
SegmentsAllowed         : {}
ExoPolicyId             : c6bf3a5d-4980-43f8-b187-f12b2b6cb2fb
SegmentsBlocked         : {Tesoreria}
SegmentAllowedFilter    :
BlockVisibility         : True
BlockCommunication      : True
State                   : Active
ObjectVersion           : b551fcbd-1e08-402b-3c25-08d9d443636e
CreatedBy               : Mario Cuomo
LastModifiedBy          : Mario Cuomo
Comment                 : Blocca la comunicazione da Segreteria a Tesoreria
ModificationTimeUtc     : 10/01/2022 14:13:34
CreationTimeUtc         : 10/01/2022 13:53:47
Identity                : FFO.extest.microsoft.com/Microsoft Exchange Hosted Organizations/cybermario.onmicrosoft.com/Configuration/Segreteria-Tesoreria
Id                      : FFO.extest.microsoft.com/Microsoft Exchange Hosted Organizations/cybermario.onmicrosoft.com/Configuration/Segreteria-Tesoreria
ExchangeVersion         : 0.20 (15.0.0.0)
Name                    : Segreteria-Tesoreria
DistinguishedName       : CN=Segreteria-Tesoreria,CN=Configuration,CN=cybermario.onmicrosoft.com,OU=Microsoft Exchange Hosted
                          Organizations,DC=FFO,DC=extest,DC=microsoft,DC=com
ObjectCategory          :
ObjectClass             : {msExchUnifiedPolicy}
WhenChanged             : 10/01/2022 15:13:34
WhenCreated             : 04/01/2022 14:47:20
WhenChangedUTC          : 10/01/2022 14:13:34
WhenCreatedUTC          : 04/01/2022 13:47:20
ExchangeObjectId        : 50ef5287-611f-4d47-ae20-3f8398110183
OrganizationalUnitRoot  : FFO.extest.microsoft.com/Microsoft Exchange Hosted Organizations/cybermario.onmicrosoft.com
OrganizationId          : FFO.extest.microsoft.com/Microsoft Exchange Hosted Organizations/cybermario.onmicrosoft.com - FFO.extest.microsoft.com/Microsoft Exchange Hosted
                          Organizations/cybermario.onmicrosoft.com/Configuration
Guid                    : 50ef5287-611f-4d47-ae20-3f8398110183
OriginatingServer       :
IsValid                 : True
ObjectState             : Unchanged
```

## Start-InformationBarrierPoliciesApplication

With this command you start the process of applying the created policies.
All policies labeled with *state=Active* are effectively *activated.*

The actual application time depends on the size of the organization.
With the tenant I created – made up of 10 users – the application time is about 20 minutes. I found a total time for the actual application in Microsoft *Teams* of about an hour.

You start the process as follows

```
Start-InformationBarrierPoliciesApplication
```

Note that if not for each pair of segments communication is not active – or blocked – in either way, the application of the command fails as follows:

```
Windows PowerShell
PS C:\Users\cuomo> Start-InformationBarrierPoliciesApplication
Your request failed to complete. Please retry. Error Details: Microsoft.Exchange.Management.Tasks.AsymmetricPoliciesException,IB Policies defined on segment
%22447c23e5-49dd-4569-a2e3-cf881b396383%22 and %22689ee7a4-4c66-4a43-891c-e43b656a947b%22 are not symmetric. Please ensure that the policies are defined two-ways. For
example, if there is a policy where Segment1 cannot communicate with Segment2, then there must be another policy where Segment2 cannot communicate with Segment1.
Status: ProtocolError
Status code: InternalServerError (500)
Status description: Internal Server Error
Response headers:
Pragma: no-cache
request-id: 833dc27b-1261-a70e-76d7-027915d1ad03
Alt-Svc: h3=":443",h3-29=":443"
X-CalculatedBETarget: PAXPR10MB4781.EURPRD10.PROD.OUTLOOK.COM
X-BackEndHttpStatus: 500
X-RUM-Validated: 1
x-ms-appId: 00000007-0000-0ff1-ce00-000000000000
X-Psws-ErrorCode: 840001
X-Psws-Exception: Microsoft.Exchange.Management.Tasks.AsymmetricPoliciesException,IB Policies defined on segment %22447c23e5-49dd-4569-a2e3-cf881b396383%22 and
%22689ee7a4-4c66-4a43-891c-e43b656a947b%22 are not symmetric. Please ensure that the policies are defined two-ways. For example, if there is a policy where Segment1
cannot communicate with Segment2, then there must be another policy where Segment2 cannot communicate with Segment1.
X-Content-Type-Options: nosniff
DataServiceVersion: 1.0;
```

If, on the other hand, the policies are well described, we are returned a *.NET* object that describes the progress of the application.

```
Windows PowerShell
PS C:\Users\cuomo> Start-InformationBarrierPoliciesApplication
WARNING: It may take several hours for the application to finish. Please check the status using Get-InformationBarrierPoliciesApplicationStatus cmdlet.
Execution of New/Set cmdlets will be prevented until start/stop is finished.


RunspaceId                : 7bbdd62b-3b43-4158-a50f-24e28c4cedc1
Identity                  : dcbbc568-2966-4e69-bfe8-f0a265ea4994
CreatedBy                 : Mario Cuomo
CancelledBy               :
Type                      : ExoApplyIBPolicyJob
ApplicationCreationTime   : 01/10/2022 14:29:21
ApplicationEndTime        :
ApplicationStartTime      : 01/10/2022 14:29:21
TotalBatches              : 0
ProcessedBatches          : 0
TotalGroupBatches         : 0
ProcessedGroupBatches     : 0
TotalGroupsToCleanup      : 0
SuccessfulCleanedupGroups : 0
FailedCleanedupGroups     : 0
PercentProgress           : 0
TotalRecipients           : 0
SuccessfulRecipients      : 0
FailedRecipients          : 0
FailureCategory           : None
Status                    : NotStarted
IsValid                   : True
ObjectState               : Unchanged
```

## Get-InformationBarrierPoliciesApplicationStatus

Once the policy application process has started, you can check its status with this command.

```
Get-InformationBarrierPoliciesApplicationStatus
```

At different times, different results are achieved.

Windows PowerShell

```
PS C:\Users\cuomo> Get-InformationBarrierPoliciesApplicationStatus


RunspaceId                : 60d29d24-7af4-433c-b1c1-e52cd39b58e5
Identity                  : dcbbc568-2966-4e69-bfe8-f0a265ea4994
CreatedBy                 : Mario Cuomo
CancelledBy               :
Type                      : ExoApplyIBPolicyJob
ApplicationCreationTime   : 01/10/2022 14:29:21
ApplicationEndTime        :
ApplicationStartTime      : 01/10/2022 14:29:21
TotalBatches              : 1
ProcessedBatches          : 1
TotalGroupBatches         : 0
ProcessedGroupBatches     : 0
TotalGroupsToCleanup      : 0
SuccessfulCleanedupGroups : 0
FailedCleanedupGroups     : 0
PercentProgress           : 100
TotalRecipients           : 8
SuccessfulRecipients      : 8
FailedRecipients          : 0
FailureCategory           : None
Status                    : PendingCompletion
IsValid                   : True
ObjectState               : Unchanged
```

Windows PowerShell

```
PS C:\Users\cuomo> Get-InformationBarrierPoliciesApplicationStatus


RunspaceId                : 60d29d24-7af4-433c-b1c1-e52cd39b58e5
Identity                  : dcbbc568-2966-4e69-bfe8-f0a265ea4994
CreatedBy                 : Mario Cuomo
CancelledBy               :
Type                      : ExoApplyIBPolicyJob
ApplicationCreationTime   : 01/10/2022 14:29:21
ApplicationEndTime        : 01/10/2022 14:48:35
ApplicationStartTime      : 01/10/2022 14:29:21
TotalBatches              : 1
ProcessedBatches          : 1
TotalGroupBatches         : 0
ProcessedGroupBatches     : 0
TotalGroupsToCleanup      : 0
SuccessfulCleanedupGroups : 0
FailedCleanedupGroups     : 0
PercentProgress           : 100
TotalRecipients           : 8
SuccessfulRecipients      : 8
FailedRecipients          : 0
FailureCategory           : None
Status                    : Completed
IsValid                   : True
ObjectState               : Unchanged
```

## INFORMATION BARRIERS FOR

*Microsoft Teams* is not the only tool affected by the application of Information *Barriers;* two other applications are *OneDrive* and *SharePoint*: mainly two tools to manage documents in the cloud. The difference is due to the fact that the first – even in its version for *Business* – has the focus on the storage of personal documents, while the second puts the emphasis on sharing and teamwork also through the creation of websites (*intra* and *extra* net).

### SHAREPOINT

By applying the criteria for information barriers to segments, it is possible to isolate websites, denying the possibility of adding users to the site and removing the possibility of viewing it – in whole or in part – to unauthorized users.

You have 4 *Information Barrier* modes that you can apply to *SharePoint* sites:

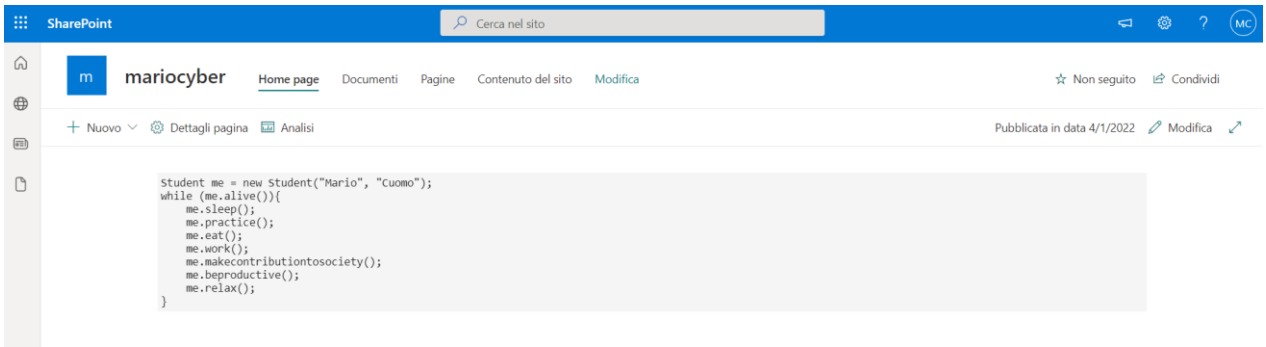
- OPEN
  it is the default mode, without restrictions.
  A user can share content based on their own barriers: if the user belongs to a segment *A* and that segment cannot communicate with segment *B,* then the user will not be able to share the content with a user in that segment.

- OWNER MODERATE
  with this mode the content of the website can only be shared between the members of the site itself.
  Only the moderator can share it externally – while respecting the constraints imposed by information barriers.

- IMPLICIT
  *implicit* mode is set by default when you assign a site to a Microsoft Teams team. This implies that the site can only be shared – as well as its content – among the users of the team itself.
  A new user can be added to the site through the Microsoft *Teams portal.*

- EXPLICIT
  *explicit* mode is set by default when you assign a site to a segment.
  The site and the content can only be shared among users in the segment.
  A new user can be added to the site only if it belongs to the associated segment.

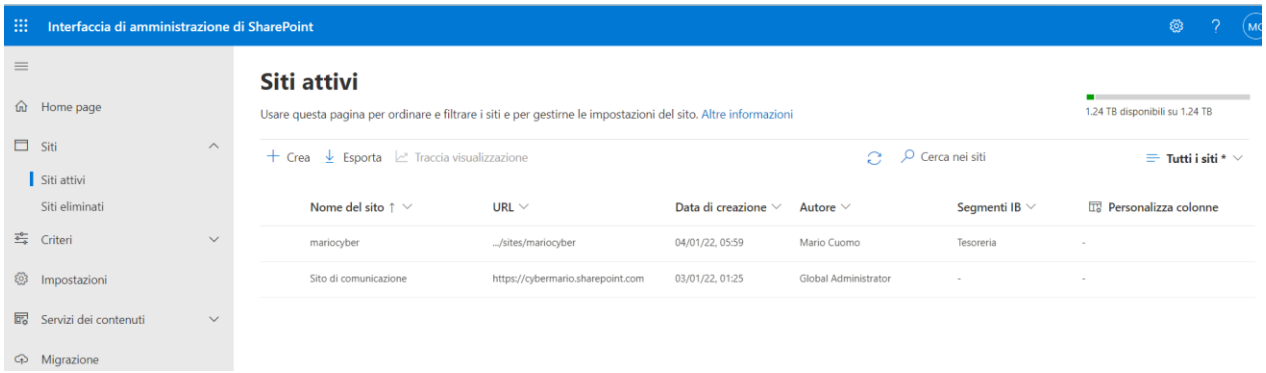
As an example, you can create a *SharePoint Online Site.*




To ensure that information barriers are also applied for *SharePoint,* you must connect to *SharePoint Online* as an administrator by using *PowerShell* and enable Information Barriers as follows:

```
Connect-SPOService -Url https://cybermario-admin.sharepoint.com -Credential
mariocuomo@cybermario.onmicrosoft.com

Set-SPOTenant -InformationBarriersSuspension $false
```

From *SharePoint* admin panel, you can set the segments to which this website belongs.




You can also do this in *PowerShell.*

```
Set-SPOSite -Identity <site URL> -AddInformationSegment <segment GUID>
```

When you assign an extension to a SharePoint site, *explicit* mode is assigned: only users of the site can access the contents of the site.

## ONEDRIVE

*Information Barriers* for *OneDrive* application prevents unauthorized collaboration by blocking access to and sharing of resources saved in storage.

There are 3 modes:

- OPEN
  is the classic mode of *OneDrive*: the user has content and can decide with whom to share it. This mode is the default when *OneDrive* has no associated segments.

- OWNER MODERATED
  in this mode only the owner can share the content of *OneDrive* to all those users who belong to segments with which communication is allowed.

- EXPLICIT
  in this mode, content can only be shared between members of the same segment as the *OneDrive* owner.

To add a segment to a *OneDrive,* you must connect to *SharePoint Online Management Shell* – as you do for *SharePoint.*
You can add up to a maximum of 100 segments.

```
Set-SPOSite -Identity <site URL> -RemoveInformationSegment <segment GUID>
```

When you add a *OneDrive* segment, you implicitly switch to explicit *mode.*

## EXTERNAL RESOURCES & REFERENCES

The material used to write this paper comes largely from the official Microsoft documentation 365 – *https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers* and the Microsoft Learn mini-guide – *https://docs.microsoft.com/it-it/learn/modules/m365-compliance-insider-plan-information-barriers*.

The use cases presented draw inspiration from the university reality of interest @Roma Tre.

*PowerShell* scripts are available in the GitHub repository at the following address *https://github.com/mariocuomo/informationBarriers-Microsoft*

Thanks to Raffaele Esposito and Biagio Davide Tinghino*(@Avanade)* for their support during the drafting of this paper.