**ELC - Azure Storage Account - Proof of Concept (POC)**

**Submitted to**

Text, logo

Description automatically generated

**By**

A logo with colorful dots

Description automatically generated

**Wipro Technologies**

**Revision History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date of Revision** | **Description of Change** | **Reason for Change** | **Reviewed By** |
| 1.1 | 09-Oct-23 | Initial Draft | NA | Syed |
| 1.2 | 19-Oct-23 | Added New Scenarios | Added the Ver 4.0 | Syed |
| 1.3 | 23-Oct-23 | Added New Scenarios | Added the Ver 5.0 | Syed |
| 1.4 | 30-Oct-23 | Added additional information. | Updated more information in All versions. | Syed |

**Author/Reviewer/Approvals**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Designation** | **Responsibility** | **Date** |
| Syed Nawazuddin | Wipro Cloud Security Engineer | Author | 09-Oct-23 |
| Kannan Kuppusamy | Wipro Technical Lead | Review by | 00-Oct-23 |
| Felix Jebamani | Wipro Lead Consultant | Review by | 00-Oct-23 |
| Jamshid Abedi | ELC ED, Global Head of Security Engineer | Approved by | 00-Oct-23 |

**Table Contents**

[1. Best Practice - Storage Account Should restrict Network Access. 4](#_Toc150245372)

[1.1 Description – 4](#_Toc150245373)

[1.2 Control Domain 4](#_Toc150245374)

[1.3 Non-Compliance Message - 4](#_Toc150245375)

[1.4 Policy Definition 4](#_Toc150245376)

[1.5 Error Details – 5](#_Toc150245377)

[1.6 Exceptions – 6](#_Toc150245378)

[2. Best Practice – Restrict Cloud Shell storage account creation. 7](#_Toc150245379)

[2.1 Description – 7](#_Toc150245380)

[2.2 Control Domain - 7](#_Toc150245381)

[2.3 Non-Compliance Message - 7](#_Toc150245382)

[2.4 Policy Definition 7](#_Toc150245383)

[2.5 Error Details – 8](#_Toc150245384)

[2.6 Exceptions – 9](#_Toc150245385)

[3. Best Practice – Require Custom tags as per org policy on resources (Enforcing). 10](#_Toc150245386)

[3.1 Description – 10](#_Toc150245387)

[3.2 Control Domain 10](#_Toc150245388)

[3.3 Non-Compliance Message - 10](#_Toc150245389)

[3.4 Policy Definition 10](#_Toc150245390)

[3.5 Error Details – 12](#_Toc150245391)

[3.6 Exceptions – 12](#_Toc150245392)

[4. Best Practice – Secure transfer to storage accounts should be enabled 14](#_Toc150245393)

[4.1 Description – 14](#_Toc150245394)

[4.2 Control Domain 14](#_Toc150245395)

[4.3 Non-Compliance Message – 14](#_Toc150245396)

[4.4 Policy Definition 14](#_Toc150245397)

[4.5 Error Details – 15](#_Toc150245398)

[4.6 Exceptions – 16](#_Toc150245399)

[5. Best Practice – Storage accounts should have infrastructure encryption. 18](#_Toc150245400)

[5.1 Description – 18](#_Toc150245401)

[5.2 Control Domain 18](#_Toc150245402)

[5.3 Non-Compliance Message – 18](#_Toc150245403)

[5.4 Policy Definition 18](#_Toc150245404)

[5.5 Error Details – 19](#_Toc150245405)

[5.6 Exceptions – 20](#_Toc150245406)

**`**

# **1. Best Practice - Storage accounts should restrict network access.**

**1.1 Description** Secure your storage account by configuring the storage firewalls and virtual networks to block all connections to the for the storage service.

**1.2 Control Domain -** Azure Security Benchmark V3.0, NIST SP 800-53 Rev. 5 Please refer to

**1.3 Non-Compliance Message** -In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended to Storage Account Should be Associated with Firewalls or Virtual Networks. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **1.4 Policy Definition**

{

  "properties": {

    "displayName": "Storage accounts should restrict network access",

    "policyType": "Custom",

    "mode": "Indexed",

    "description": "Network access to storage accounts should be restricted. Configure network rules so only applications from allowed networks can access the storage account. To allow connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges",

    "metadata": {

      "category": "Storage",

      "createdBy": "0a27dc35-c333-4a9b-81de-4601b40fac2a",

      "createdOn": "2023-10-05T07:11:16.3692863Z",

      "updatedBy": null,

      "updatedOn": null

    },

    "parameters": {

      "effect": {

        "type": "String",

        "metadata": {

          "displayName": "Effect",

          "description": "The effect determines what happens when the policy rule is evaluated to match"

        },

        "allowedValues": [

          "Audit",

          "Deny",

          "Disabled"

        ],

        "defaultValue": "Deny"

      }

    },

    "policyRule": {

      "if": {

        "allOf": [

          {

            "field": "type",

            "equals": "Microsoft.Storage/storageAccounts"

          },

          {

            "field": "Microsoft.Storage/storageAccounts/networkAcls.defaultAction",

            "notEquals": "Deny"

          }

        ]

      },

      "then": {

        "effect": "[parameters('effect')]"

      }

    }

  },

**1.5 Error Details –** The location of the error details depends on what aspect of Azure Policy you're working with & error summary details.

A screenshot of a computer

Description automatically generated

Figure 1 - Validation Failed error summary details.

**1.6 Exceptions –** While creating or after created the policy, We can Exclusions the Subscription/Resource Group/ Resource.

A screenshot of a computer

Description automatically generated

Figure 2 - Select the policy, Click on Create Exemption.

A screenshot of a computer

Description automatically generated

Figure 3 - Select the Exemption Scope (Subscription/ Resource Group / Resource).

# **2. Best Practice – Restrict Cloud Shell storage account creation.**

**2.1 Description –** Azure Cloud Shell is an interactive, authenticated, browser-accessible terminal for managing Azure resources. It provides the flexibility of choosing the shell experience that best suits the way you work, either Bash or PowerShell. Cloud Shell runs on a temporary host provided on a per-session, per-user basis.

**2.2 Control Domain -** Custom Policy.

**2.3 Non-Compliance Message -** In accordance with ELC IT-Security & Compliance, it is recommended to Storage Account Should not be created with the Cloud Shell. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **2.4 Policy Definition**

{

"displayName":"Restrict cloud shell storage account creation",

"description":"Storage accounts that you create in Cloud Shell are tagged with ms-resource-usage:azure-cloud-shell. If you want to disallow users from creating storage accounts in Cloud Shell, create an Azure resource policy for tags that is triggered by this specific tag. https://learn.microsoft.com/en-us/azure/cloud-shell/persisting-shell-storage#restrict-resource-creation-with-an-azure-resource-policy",

"metadata":

{

    "category":"Tags",

    "version":"1.0.0"

    },

    "mode":"All",

    "parameters":{

        "effect":{

            "type":"String",

            "metadata":{

                "displayName":"Effect",

                "description":"Enable or disable the execution of the policy"

                },

                "allowedValues":[

                    "Deny",

                    "Audit",

                    "Disabled"],

                    "defaultValue":"Deny"

                    }

                    },

    "policyRule":{

        "if":{

            "allOf":[

                {

                    "field":"type",

                    "equals":"Microsoft.Storage/storageAccounts"

                    },

                    {

                    "field":"tags['ms-resource-usage']",

                    "equals":"azure-cloud-shell"

                    }

                    ]

                    },

"then":{

"effect":"[parameters('effect')]"

        }

    }

}

**2.5 Error Details –** The location of the error details depends on what aspect of Azure Policy you're working with & error summary details.

A screenshot of a computer error

Description automatically generated

**2.6 Exceptions –** While creating or after created the policy, We can Exclusions the Subscription/Resource Group/ Resource.

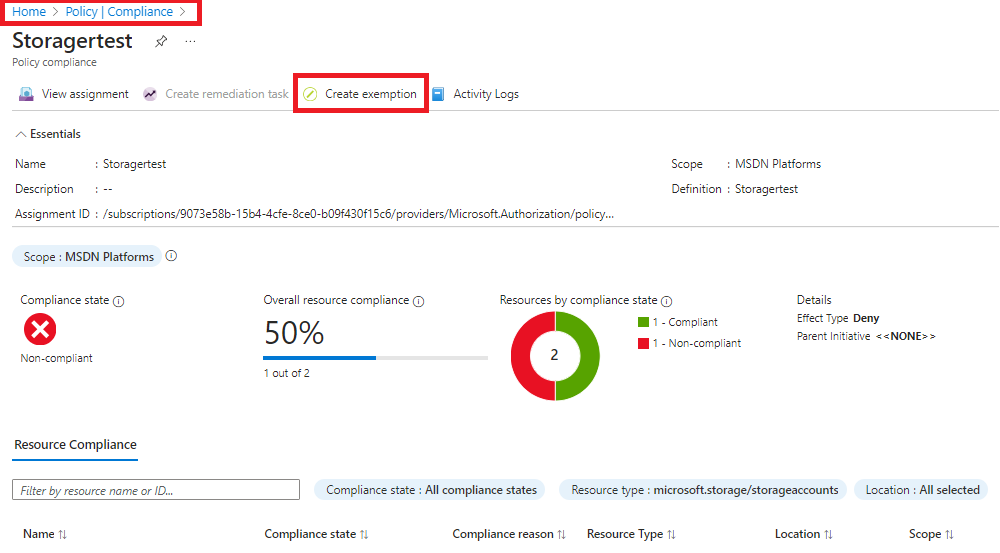


Figure 4 - Select the policy, Click on Create Exemption.

A screenshot of a computer

Description automatically generated

Figure 5 - Select the Exemption Scope (Subscription/ Resource Group / Resource).

# **3. Best Practice – Require Custom tags as per org policy on resources (Enforcing).**

**3.1 Description –** Tags are an important part of managing, organizing, and governing your Azure resources.

1. They can help you keep track of Azure resources, manage access control, assign bulk Azure automation actions to resources with the same tag name, and manage costs and budgets.
2. Tags can be used to organize Azure resources into a taxonomy. They can also help locate resources within the console and report costs associated with different projects. Additionally, tags can be used to support role-based permissions and identify patterns and assets required to support workloads.

Azure Policy makes it possible to configure tags on your new and existing resources at scale with the modify effect and remediation tasks. By using an Azure Policy, you can avoid the scenario of resources being deployed to your subscription that don’t have the expected tags for your organization. Instead of manually applying tags or searching for resources that aren’t compliant, you create a policy that automatically applies the needed tags during deployment.

**3.2 Control Domain -** Custom Policy.

**3.3 Non-Compliance Message** -Required tag as per the Organization Policy - Application Name, Application Owner, Application ID, Application Description, Business Owner, Cost Center, Department, Environment, Location, Project ID, Region, Date, Fiscal Year. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **3.4 Policy Definition**

Note – We can change the tags as per the organization needs.

{

    "displayName": "Require custom tags as per org policy on resources",

    "policyType": "BuiltIn",

    "mode": "Indexed",

    "description": "Enforces existence of a tag. Does not apply to resource groups.Enforce each resource to be tagged as per the organizational cloud governance policy",

    "metadata": {

      "version": "1.0.1",

      "category": "Tags"

    },

    "policyRule": {

      "if": {

        "allOf": [

          {

            "field": "tags[Application Name]",

            "exists": "false"

          },

          {

            "field": "tags[Application Owner]",

            "exists": "false"

          },

          {

            "field": "tags[Application ID]",

            "exists": "false"

          },

          {

            "field": "tags[Application Description]",

            "exists": "false"

          },

          {

            "field": "tags[Business Owner]",

            "exists": "false"

          },

          {

            "field": "tags[Cost Centre]",

            "exists": "false"

          },

          {

            "field": "tags[Department]",

            "exists": "false"

          },

          {

            "field": "tags[Environment]",

            "exists": "false"

          },

          {

            "field": "tags[Location]",

            "exists": "false"

          },

          {

            "field": "tags[Project ID]",

            "exists": "false"

          },

          {

            "field": "tags[Region]",

            "exists": "false"

          },

          {

            "field": "tags[Date]",

            "exists": "false"

          },

          {

            "field": "tags[Fiscal Year]",

            "exists": "false"

          }

        ]

      },

      "then": {

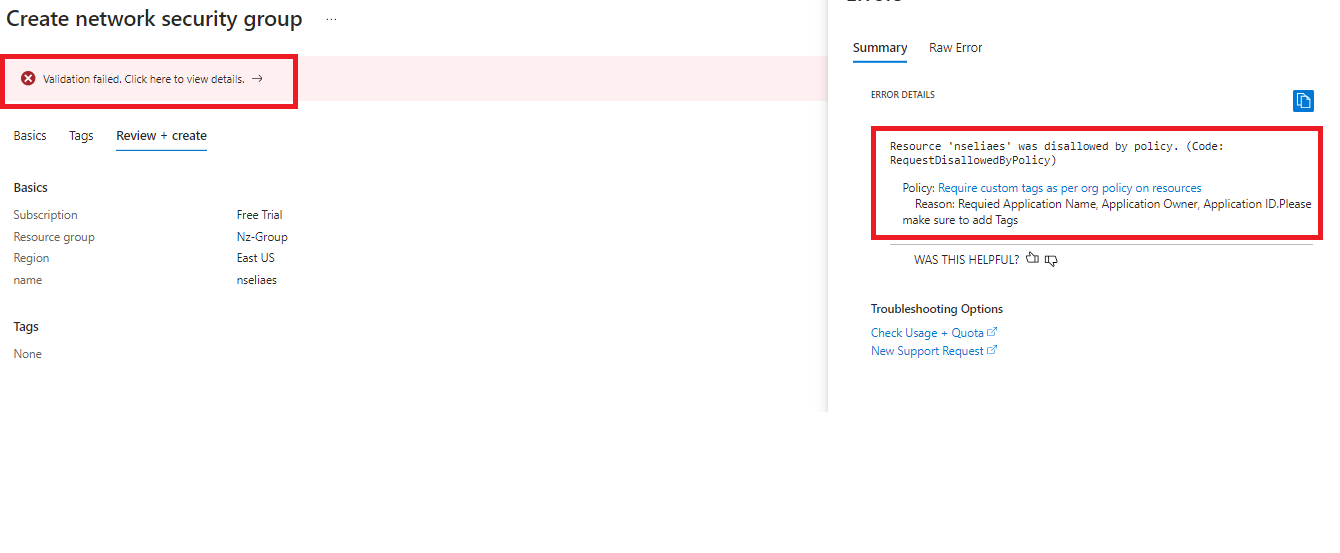
        "effect": "deny"

      }

    }

  }

**3.5 Error Details –** The location of the error details depends on what aspect of Azure Policy you're working with & error summary details.



**3.6 Exceptions –** While creating or after created the policy, We can Exclusions the Subscription/Resource Group/ Resource.

A screenshot of a computer

Description automatically generated

Figure 2 - Select the policy, Click on Create Exemption.

A screenshot of a computer

Description automatically generated

Figure 3 - Select the Exemption Scope (Subscription/ Resource Group / Resource).

# **4. Best Practice – Secure transfer to storage accounts should be enabled**

**4.1 Description –** Secure transfer is an option that forces your storage account to accept requests only from secure connections (HTTPS). Use of HTTPS ensures authentication between the server and the service and protects data in transit from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking.

**4.2 Control Domain -** CIS V1.4.0

**4.3 Non-Compliance Message** –Storage Account should be Secure transfer in your storage account. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **4.4 Policy Definition**

{

  "properties": {

    "displayName": "Secure transfer to storage accounts should be enabled",

    "policyType": "BuiltIn",

    "mode": "Indexed",

    "description": "Audit requirement of Secure transfer in your storage account. Secure transfer is an option that forces your storage account to accept requests only from secure connections (HTTPS). Use of HTTPS ensures authentication between the server and the service and protects data in transit from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking",

    "metadata": {

      "version": "2.0.0",

      "category": "Storage"

    },

    "version": "2.0.0",

    "parameters": {

      "effect": {

        "type": "string",

        "defaultValue": "Deny",

        "allowedValues": [

          "Audit",

          "Deny",

          "Disabled"

        ],

        "metadata": {

          "displayName": "Effect",

          "description": "The effect determines what happens when the policy rule is evaluated to match"

        }

      }

    },

    "policyRule": {

      "if": {

        "allOf": [

          {

            "field": "type",

            "equals": "Microsoft.Storage/storageAccounts"

          },

          {

            "anyOf": [

              {

                "allOf": [

                  {

                    "value": "[requestContext().apiVersion]",

                    "less": "2019-04-01"

                  },

                  {

                    "field": "Microsoft.Storage/storageAccounts/supportsHttpsTrafficOnly",

                    "exists": "false"

                  }

                ]

              },

              {

                "field": "Microsoft.Storage/storageAccounts/supportsHttpsTrafficOnly",

                "equals": "false"

              }

            ]

          }

        ]

      },

      "then": {

        "effect": "[parameters('effect')]"

      }

    }

  }

}

**4.5 Error Details –** The location of the error details depends on what aspect of Azure Policy you're working with & error summary details.

Note – To find the error Go to Storage Account > Configuration > Secure transfer Required.

A screenshot of a computer screen

Description automatically generated

**4.6 Exceptions –** While creating or after created the policy, We can Exclusions the Subscription/Resource Group/ Resource.

A screenshot of a computer

Description automatically generated

Figure 2 - Select the policy, Click on Create Exemption.

A screenshot of a computer

Description automatically generated

Figure 3 - Select the Exemption Scope (Subscription/ Resource Group / Resource).

# **5. Best Practice – Storage accounts should have infrastructure encryption.**

**5.1 Description –** Double encryption of Azure Storage data protects against a scenario where one of the encryption algorithms or keys may be compromised. In this scenario, the additional layer of encryption continues to protect your data. Enable infrastructure encryption for higher level of assurance that the data is secure. When infrastructure encryption is enabled, data in a storage account is encrypted twice.

**Note** – Once the encryption is enabled cannot be disable.

**5.2 Control Domain -** NIST SP 800-53 Rev. 5

**5.3 Non-Compliance Message** –Storage Account should have Infrastructure encryption, Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **5.4 Policy Definition**

{

    "properties": {

      "displayName": "Storage accounts should have infrastructure encryption",

      "policyType": "BuiltIn",

      "mode": "Indexed",

      "description": "Enable infrastructure encryption for higher level of assurance that the data is secure. When infrastructure encryption is enabled, data in a storage account is encrypted twice.",

      "metadata": {

        "version": "1.0.0",

        "category": "Storage"

      },

      "parameters": {

        "effect": {

          "type": "String",

          "metadata": {

            "displayName": "Effect",

            "description": "Enable or disable the execution of the audit policy"

          },

          "allowedValues": [

            "Audit",

            "Deny",

            "Disabled"

          ],

          "defaultValue": "Deny"

        }

      },

      "policyRule": {

        "if": {

          "allOf": [

            {

              "field": "type",

              "equals": "Microsoft.Storage/storageAccounts"

            },

            {

              "field": "Microsoft.Storage/storageAccounts/encryption.requireInfrastructureEncryption",

              "notEquals": "true"

            }

          ]

        },

        "then": {

          "effect": "[parameters('effect')]"

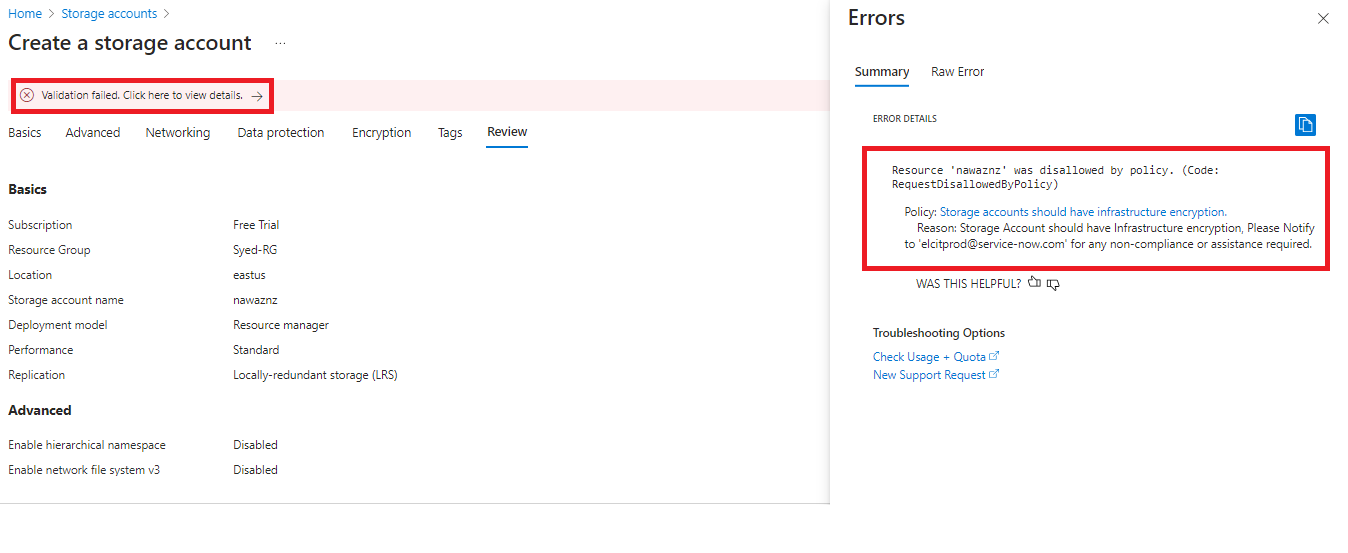
        }

      }

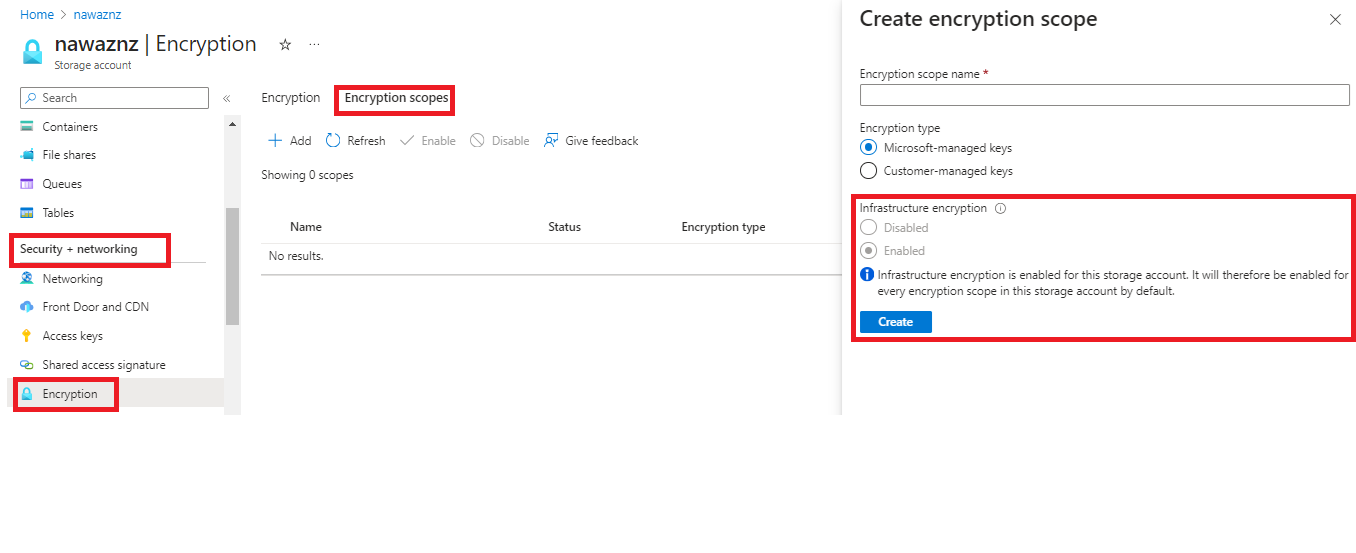
    }

}

**5.5 Error Details –** The location of the error details depends on what aspect of Azure Policy you're working with & error summary details.



Note – To find the error Go to Storage Account > security +Networking > Encryption > Encryption Scopes > **infrastructure encryption**.



**5.6 Exceptions –** While creating or after created the policy, We can Exclusions the Subscription/Resource Group/ Resource.

A screenshot of a computer

Description automatically generated

Figure 2 - Select the policy, Click on Create Exemption.

A screenshot of a computer

Description automatically generated

Figure 3 - Select the Exemption Scope (Subscription/ Resource Group / Resource).

**Objective of the Document**

In accordance with the Global Information Security Policy, an Azure storage account to ensure that Estee Lauder Companies Inc. (ELC) can capture and analyse activity within the Azure cloud environment effectively and efficiently. It also helps provide the sufficient detection and identification capabilities needed to support information security. This procedure enables the technology controls and processes needed to ensure transparency and auditability across the technology environment, which will empower ELC’s ability to perform investigations, regulatory audits, incident, and problem management, etc.

**Executive Summary**

In any IT industry, data plays an important role. Every day there are new ways to steal, or valuable data gets compromised. To overcome this, we should build and configure strong monitoring and logging in our environment to address the everyday challenges we are facing in securing our corporate information. There are several tools and technologies available, and we are making use of them to safeguard our data and information integrity. In this document, we are focusing on the Azure policy service to monitor our Azure resources and their logs.

**6. Appendix**

6.1 Reference Links.

* <https://learn.microsoft.com/en-us/azure/storage/common/infrastructure-encryption-enable?tabs=portal>
* <https://learn.microsoft.com/en-us/azure/governance/policy/samples/cis-azure-1-4-0>