**CORE SERVICE DESIGN:**

**Azure Policy**

atabricks

|  |  |
| --- | --- |
| IT Owner Details | |
| **Department** | DTS |
| **Contact Name** | Dominic Panzera |
| **Address** | 375 Manningham Road, Doncaster, Victoria 3108 |

|  |  |
| --- | --- |
| Document Control | |
| Title | Ambulance Victoria – Azure Policy Core Service Design |
| **File Name** | Ambulance Victoria – Azure Policy Core Service Design v1.0.docx |
| **Version** | 1.0 |
| **Status** | Draft |
| **Release Date** |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Preparation |  |  | |  | |
| **Prepared** | Arshdeep Singh |  | |  | |
| **Authorised** |  | |  | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Tracking | | | |  |
| Version | Remarks | Change Requested | Pages Affected | Release Date |
| 1.0 | Initial Release | N/A | All |  |

Table of Contents

[1. Overview 5](#_Toc151034051)

[1.1 Purpose and Audience 5](#_Toc151034052)

[1.2 Scope and Key Deliverables 5](#_Toc151034053)

[1.3 Glossary and Definitions 6](#_Toc151034054)

# Overview

This document covers the baseline design for the Azure Policy core service. The intention of this document is to define the overall resource design in isolation from a specific application. It is aimed to highlight the general process and requirements for building a Azure Policy in a repeatable fashion with consistent configurations. Design decisions and justifications have been included in the Architecture section, and this document can be used as a reference for new builds that require a Azure Policy.

This design caters to a Level 2 design which covers both Microsoft’s WAF (Well Architected Framework)[[1]](#footnote-2) and the Department of Health Control list.

Any deviations required to the standards defined in this document will require separate exemption and approval from the Cloud Governance Forum if they are required for any reason for a specific build.

## Purpose and Audience

This document will outline the standard design and configuration of this Azure service in Ambulance Victoria’s Azure tenancy as a baseline for any application infrastructure deployments.

This design is intended to:

* Meet Microsoft WAF standards.
* Meet the controls stipulated by the Department of Health.
* Define the baseline required for the deployment of the resource.

The audience for this document is those involved in the planning, designing, and implementing of the Application/Data infrastructure. This includes:

* + Ambulance Victoria IT staff

It is assumed that the reader knows and is familiar with Azure Cloud concepts and related topics.

## Scope and Key Deliverables

The scope of this core service design is to define the baseline deployment requirements and standards for the Azure Policy core service.

The key deliverables for this are:

* This design to outline the service definition Level 2 baseline standards.
* A technical configuration document that defines the deployment of this resource for each of the Service Tiers, or for any other logical standard such as size
* IaC templates for repeatable deployment of this core service

## Glossary and Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **AV** | Ambulance Victoria |
| **WAF** | Well Architected Framework |
| **CAF** | Cloud Adoption Framework |
| **Level 1** | Refers to a resource that has been designed to a CAF standard |
| **Level 2** | Refers to a resource that has been designed to a WAF standard with Department of Health controls overlayed |
| **AZ 2** | Refers to Ambulance Victoria’s legacy Azure Landing Zone still in use in some regards |
| **AZ 3** | Refers to Ambulance Victoria’s current Azure Landing Zone, also referred to as the Enterprise landing zone. This is the target state for migrations. |
| **SLA** | Service Level Agreement as defined by Microsoft |
| **DH** | Department of Health |
| **IaC** | Infrastructure as Code |
| **NSG** | Network Security Groups |

Table 1: Glossary and definitions

# Alerting

There are no additional Azure Policies required.

# App Gateway

There are no additional Azure Policies required for this service.

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

The following Microsoft Security Benchmark controls are applicable:

* NS-1: Establish network segmentation boundaries
* NS-2: Secure cloud services with network controls
* IM-8: Restrict the exposure of credential and secrets
* DP-3: Encrypt sensitive data in transit
* DP-7: Use a secure certificate management process
* LT-4: Enable logging for security investigation

# App Services

The following policies will be applied for the Azure App Service. These are all built-in policies that can be enabled to audit, then enforce when ready:

|  |  |
| --- | --- |
| Policy Name | Description |
| App Service apps should have 'Client Certificates (Incoming client certificates)' enabled | Client certificates allow for the app to request a certificate for incoming requests. Only clients that have a valid certificate will be able to reach the app. |
| App Service apps should have remote debugging turned off | Remote debugging requires inbound ports to be opened on an App Service app. Remote debugging should be turned off. |
| App Service apps should not have CORS configured to allow every resource to access your apps | Cross-Origin Resource Sharing (CORS) should not allow all domains to access your app. Allow only required domains to interact with your app. |
| App Service apps should only be accessible over HTTPS | Use of HTTPS ensures server/service authentication and protects data in transit from network layer eavesdropping attacks. |
| App Service apps should require FTPS only | Enable FTPS enforcement for enhanced security. |
| App Service apps should use the latest TLS version | Periodically, newer versions are released for TLS either due to security flaws, include additional functionality, and enhance speed. Upgrade to the latest TLS version for App Service apps to take advantage of security fixes, if any, and/or new functionalities of the latest version. |

Table 8: Additional Azure Policies to be deployed for this service

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

The following Microsoft Security Benchmark controls are applicable:

* NS-1: Establish network segmentation boundaries
* NS-2: Secure cloud services with network controls
* NS-5: Deploy DDOS protection
* NS-6: Deploy web application firewall
* IM-3: Manage application identities securely and automatically
* IM-8: Restrict the exposure of credential and secrets
* DP-3: Encrypt sensitive data in transit
* DP-4: Enable data at rest encryption by default
* DP-7: Use a secure certificate management process
* LT-1: Enable threat detection capabilities
* LT-4: Enable logging for security investigation
* BR-1: Ensure regular automated backups
* PV-2: Audit and enforce secure configurations
* DS-6: Enforce security of workload throughout DevOps lifecycle

https://learn.microsoft.com/en-us/azure/well-architected/security/security-principles

# Bastion

The only required exemption to standard policies is for the Deny Public IP Policy to be removed so that the Public IP for Bastion can be deployed. Note that this is already in place based on the current deployment.

<https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/azure-bastion-security-baseline>

### Azure Policy Security Checklist

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | DH Ref. | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **S1** | 3.2.4 | Administrative activities are conducted through jump servers. | Yes | Yes | Already deployed - Bastion | Operational |

Table 4: Security checklist summary

https://learn.microsoft.com/en-us/azure/well-architected/security/security-principles

# Data Factory

There are no additional Azure Policies required for this service.

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

The following Microsoft Security Benchmark controls are applicable:

* NS-1: Establish network segmentation boundaries
* NS-2: Secure cloud services with network controls
* IM-1: Use centralized identity and authentication system
* IM-3: Manage application identities securely and automatically
* DP-3: Encrypt sensitive data in transit
* DP-4: Enable data at rest encryption by default
* LT-4: Enable logging for security investigation
* BR-1: Ensure regular automated backups

# Azure File Services

There are no Azure Policies required to support this service.

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

The following Microsoft Security Benchmark controls are applicable:

* NS-2: Secure cloud services with network controls
* IM-1: Use centralized identity and authentication system
* DP-3: Encrypt sensitive data in transit
* DP-4: Encrypt sensitive data at rest
* LT-1: Enable threat detection capabilities
* LT-4: Enable logging for security investigation
* BR-1: Ensure regular automated backups

# Firewall

There are no Azure Policies required to support this service.

### Azure Policy Reliability Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Design | Enforcement Option | Applicability |
| **R1** | Use Azure Firewall Manager with traditional Hub & Spokes or Azure Virtual WAN network topologies to deploy and manage instances of Azure Firewall. | Yes | Yes | IaC | At deployment |
| **R2** | Create Azure Firewall Policies to govern the security posture across global network environments. Assign policies to all instances of Azure Firewall. | Yes | Yes | IaC | At deployment |
| **R3** | Migrate Azure Firewall Classic Rules to Azure Firewall Manager Policies for existing deployments. | No – classic rules not used | No | N/A | N/A |
| **R4** | Review the list of Azure Firewall Known Issues. | Yes | No | Governance | Operational – review quarterly |
| **R5** | Ensure your Azure Firewall Policy adheres to Azure Firewall limits and recommendations. | Yes | No | Governance | Operational – review monthly |
| **R6** | Deploy Azure Firewall across multiple availability zones for higher service-level agreement (SLA). | Yes | No | IaC | N/A – Availability Zones not available in Primary Region |
| R7 | In multi-region environments, deploy an Azure Firewall instance per region. | Yes | Yes | IaC | At deployment |
| **R8** | Monitor Azure Firewall Metrics and Resource Health state. | Yes | Yes | IaC | At deployment |

The following Department of Health control is required to be met above and beyond the Microsoft Security Benchmark:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | DH ID | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **S1** | 12.3.1 | Configure trusted DNS servers on enterprise assets. Example implementations include: configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers. | Yes | No | IaC | At deployment |

# Load Balancer

There are no Azure Policies relevant for this resource.

<https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-floating-ip>

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

The following Microsoft Security Benchmark controls are applicable to this service:

* NS-1 Establish network segmentation boundaries
* LT-4 Enable network logging for security investigation

There are no Department of Health controls above and beyond the Azure Security Benchmark for Azure Load Balancer.

# Monitor and Insights

There are no specific Azure Policies required for these services.

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

The following Microsoft Security Benchmark controls are applicable to Azure Monitor[[2]](#footnote-3):

* IM-1: Use centralized identity and authentication system.
* IM-3: Manage application identities securely and automatically.
* DP-3: Encrypt sensitive data in transit.
* DP-4: Enable data at rest encryption by default.
* LT-4: Enable logging for security investigation.

# Network Gateway

There are no specific Azure Policies required that relate to Azure Virtual Network Gateway.

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

The relevant Microsoft Security Controls include the following:

* DP-3: Encrypt sensitive data in transit
* LT-4: Enable logging for security investigation
* AM-2 Use only approved services

# Site Recovery

The following built-in Azure Policy may be used if it is preferable to using PowerShell during deployments:

|  |  |
| --- | --- |
| Policy Name | Description |
| Configure disaster recovery on virtual machines by enabling replication via Azure Site Recovery | Virtual machines without disaster recovery configurations are vulnerable to outages and other disruptions. If the virtual machine does not already have disaster recovery configured, this would initiate the same by enabling replication using preset configurations to facilitate business continuity. You can optionally include/exclude virtual machines containing a specified tag to control the scope of assignment. |

For this Policy it is recommended to apply to Production Virtual Machines. The settings within this policy can be configured so that only machines with a specific tag will have this enabled. As discussed in this document, ASR is not recommended to be the default enablement across all servers, only specific servers that have this as a requirement.

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

### Azure Policy Security Checklist

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | DH Ref. | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **S1** | 19.1.1 | Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | Yes | No | Governance | Operational - annually |
| **S2** | 19.2.2 | Maintain a physically separate recovery site that enables ready restoration of key systems in the event that their availability is lost. | Yes | Yes | IaC | At deployment |
| **S3** | 5.1.2 | Restoration of important data, software and configuration settings from backups to a common point of time is tested as part of disaster recovery exercises. | Yes | No | Governance | Operational – quarterly |
| **S4** | 19.1.3 | Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets. | Yes | No | Governance | Operational - quarterly |

Table 7: Security checklist summary

# SQL DB

The following policies should be applied to audit or enforce the configurations for Azure SQL Database:

|  |  |
| --- | --- |
| Policy Name | Scope |
| Private endpoint connections on Azure SQL Database should be enabled | av (root management group) |
| Public network access on Azure SQL Database should be disabled | av (root management group) |
| An Azure Active Directory administrator should be provisioned for SQL servers | av (root management group) |
| Azure SQL Database should have Azure Active Directory Only Authentication enabled | av (root management group) |
| Transparent Data Encryption on SQL databases should be enabled | av (root management group) |
| Auditing on SQL server should be enabled | av (root management group) |

Table 9: Azure Policies

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

The following Microsoft Security Benchmark Controls are applicable:

* NS-1: Establish network segmentation boundaries
* NS-2: Secure cloud services with network controls
* IM-1: Use centralized identity and authentication system
* DP-3: Encrypt sensitive data in transit
* DP-4: Enable data at rest encryption by default
* LT-1: Enable threat detection capabilities
* LT-3: Enable logging for security investigation
* LT-4: Enable logging for security investigation
* BR-1: Ensure regular automated backups

# SQL Managed Instance

The following Azure policies should be applied:

|  |  |
| --- | --- |
| Policy Name | Scope |
| Azure Defender for SQL should be enabled for unprotected SQL Managed Instances | av management group (under Root) |

Table 10: Azure Policies

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

The following Microsoft Security Benchmark Controls are applicable:

* NS-1: Establish network segmentation boundaries
* IM-1: Use centralized identity and authentication system
* IM-3: Manage application identities securely and automatically
* DP-3: Encrypt sensitive data in transit
* DP-4: Enable data at rest encryption by default

# Update Manager

The following Policies should be applied for this service:

|  |  |
| --- | --- |
| Policy Name | Scope |
| Configure periodic checking for missing system updates on Azure virtual machines | av management group (under Root) |
| Schedule recurring updates using Azure Update Manager | av management group (under Root) |

Table 5: Azure Policies

### Azure Policy Security Checklist

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | DH Ref. | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **S1** | 4.1.1 | Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. | Yes | No | Governance | Operational – as required |
| **S2** | 4.1.2 | Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within one month of release. | Yes | Yes | IaC | At deployment |
| **S3** | 4.2.1 | Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within two weeks of release. | Yes | Yes | IaC | At deployment |
| **S4** | 4.3.1 | Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within 48 hours if an exploit exists. | Yes | No | Governance | Operational – as reuqired |
| **S5** | 15.2.5 | Perform Automated Operating System & Application Patch Management | Yes | Yes | IaC | At deployment |

Table 3: Security checklist summary

# Cosmos DB

There are no additional Azure Policies required for this service.

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

The following Microsoft Security Benchmarks are applicable:

* NS-1: Establish network segmentation boundaries
* NS-2: Secure cloud services with network controls
* IM-3: Manage application identities securely and automatically
* DP-2: Monitor anomalies and threats targeting sensitive data
* DP-3: Encrypt sensitive data in transit
* DP-4: Enable data at rest encryption by default
* LT-1: Enable threat detection capabilities
* LT-4: Enable logging for security investigation
* BR-1: Ensure regular automated backups

# DDoS

The following Azure policy should be applied:

|  |  |
| --- | --- |
| Policy Name | Scope |
| Public IP addresses should have resource logs enabled for Azure DDoS Protection | av management group (under tenant root) |

Table 6: Azure Policies

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

The Microsoft Security Benchmark controls that apply are:

* LT-4: Enable logging for security investigation

There are no Department of Health controls above and beyond the Microsoft Security Benchmark.

# Defender for Cloud

The following Azure Policies will be applied to enable Defender on subscriptions as they are created:

|  |  |
| --- | --- |
| Policy Name | Scope |
| Azure Defender for App Service should be enabled | av management group |
| Azure Defender for Azure SQL Database servers should be enabled | av management group |
| Azure Defender for Key Vault should be enabled | av management group |
| Azure Defender for open-source relational databases should be enabled | av management group |
| Azure Defender for Resource Manager should be enabled | av management group |
| Azure Defender for servers should be enabled | av management group |
| Azure Defender for SQL servers on machines should be enabled | av management group |
| Azure Defender for SQL should be enabled for unprotected Azure SQL servers | av management group |
| Azure Defender for SQL should be enabled for unprotected PostgreSQL flexible servers | av management group |
| Azure Defender for SQL should be enabled for unprotected SQL Managed Instances | av management group |
| Azure Defender for Storage should be enabled | av management group |
| Azure Defender for Kubernetes should be enabled | av management group |
| Azure Defender for container registries should be enabled | av management group |

Table 5: Azure Policies

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

### Azure Policy Security Checklist

There is no specific guidance for Defender for Cloud. However, it supports meeting the following Microsoft Security Benchmark items across all supported resources:

* LT-1 Enable threat detection.

# Event Hub

There are no additional Azure Policies required for Event Hubs.

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

The following Microsoft Security Benchmark guidelines apply[[3]](#footnote-4):

* NS-1: Establish network segmentation boundaries
  + Private Network injection
  + Service Tags
* NS-2: Secure cloud services with network controls
  + Private Endpoints
* IM-1: Use centralized identity and authentication system
* IM-3: Manage application identities securely and automatically
* PA-1: Separate and limit highly privileged/administrative users
* PA-7: Follow just enough administration (least privilege) principle
* DP-3: Encrypt sensitive data in transit
* DP-4: Enable data at rest encryption by default
* LT-4: Enable logging for security investigation

There are no Department of Health controls above and beyond the Microsoft Security Benchmark for this service.

# Express Route

There are no Azure Policies required for this service.

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

The following Microsoft Security Benchmark Controls are applicable:

* LT-4: Enable logging for security investigation.

# KeyVault

There are some already existing policies for Key Vault in the Ambulance Victoria tenancy:

|  |  |
| --- | --- |
| Policy Name | Scope |
| Configure Azure Defender for Key Vaults to be enabled | av management group (under root) |
| Key vaults should have soft delete enabled | av management group (under root) |

Table 8: Existing Azure Policies

The following policies are to be implemented and are all built-in policies:

|  |  |  |
| --- | --- | --- |
| Policy Name | Definition | Scope |
| Azure Key Vault should have Firewall enabled | Enable the key vault firewall so that the key vault is not accessible by default to any public IPs. Optionally, you can configure specific IP ranges to limit access to those networks. | av management group (under root) |
| Azure Key Vaults should use private link | Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to key vault, you can reduce data leakage risks. | av management group (under root) |
| Key vault keys should have an expiration date | Cryptographic keys should have a defined expiration date and not be permanent. Keys that are valid forever provide a potential attacker with more time to compromise the key. It is a recommended security practice to set expiration dates on cryptographic keys. | av management group (under root |
| Key vault secrets should have an expiration date | Secrets should have a defined expiration date and not be permanent. Secrets that are valid forever provide a potential attacker with more time to compromise them. It is a recommended security practice to set expiration dates on secrets. | av management group (under root |

Table 8: Additional Azure Policies

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

The following Microsoft Security Benchmark Controls are relevant to Key Vaults[[4]](#footnote-5):

* NS-1: Establish network segmentation boundaries.
* NS-2: Secure cloud services with network controls
  + Use Private Endpoints
  + Disable Public Access
  + Defender Monitoring via Azure Policy
* IM-3: Manage application identities securely and automatically.
* IM-8: Restrict the exposure of credential and secrets.
* DP-3: Encrypt sensitive data in transit.
* DP-4: Enable data at rest encryption by default.
* DP-6: Use a secure key management process.
  + Key Vault keys should have an expiration date.
  + Key Vault secrets should have an expiration date.
* DP-7: Use a secure certificate management process.
  + [Preview]: Certificates should have the specified maximum validity period.
* LT-1: Enable threat detection capabilities.
* LT-4: Enable logging for security investigation.
* BR-1: Ensure regular automated backups.

### Azure Policy Security Checklist

There is only one Department of Health control that is not covered by the Microsoft Security Baseline:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | DH Ref. | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **S1** | 19.2.2 | Maintain a physically separate recovery site that enables ready restoration of key systems in the event that their availability is lost. | Yes | Yes | Default | At deployment |

Table 6: Security checklist summary

# Log Analytics Workspace

Though this policy does not specifically apply to the Log Analytics Workspace, it sets diagnostic settings for all resources in that region through Azure Policy so that they do not need to be coded or applied at deployment each time.

|  |  |
| --- | --- |
| Policy Name | Scope |
| Deploy-Resource-Diag-Australia-Southeast | av management group (under Root) |
| Deploy-Resource-Diag-Australia-East | av management group (under Root) |

Table 6: Azure Policies

Note that for any resources not listed, thought the IaC templates will have the capability to deploy them, it is also best to add that resource into the policies above so that this can be done by Policy and reduce the dependency on having this defined in IaC templates. The following resources are included in the above policies:

* NSG
* Public IP
* Application Gateway
* Time Series Insights
* Cognitive Services
* Data Lake Analytics
* Virtual Machines
* Azure Data Explorer Cluster
* App Service
* Event Grid System Topic
* Virtual Network
* Analysis Services
* SQL Elastic Pools
* Stream Analytics
* Power BI Embedded
* Event Grid Topic
* Traffic Manager
* Search Services
* Azure Data Lake Store
* Storage Accounts
* ExpressRoute
* Load Balancer
* CDN Endpoint
* Logic Apps
* Event Grid Subscriptions
* Network Interfaces
* ML Workspaces
* Logic Apps
* Data Factory
* Azure Function App
* WVD
* PostgreSQL
* Service Bus
* App Service Plan
* Automation Accounts
* Databricks
* Redis Cache
* Azure Media Service
* Front Door
* HD Insight
* Key Vault
* Firewall
* Event Hubs
* Azure API for FHIR
* APIM
* MariaDB
* SignalR
* Cosmos DB
* VPN Gateway
* SQL DB
* IOT
* MySQL DB
* Virtual Machines Scale Sets
* SQL Managed Instances
* Container Registry
* Kubernetes
* Container Instances

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

### Azure Policy Security Checklist

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | DH Ref. | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **S1** | 16.1.1 | Establish and maintain an audit log management and monitoring process that defines the enterprise’s logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | Yes | No | Governance | Operational – review quarterly |
| **S2** | 16.2.1 | Collect audit logs and ensure adequate audit log storage for critical servers, workstations, laptops and other devices and stored securely. | Yes | Yes | IaC | At deployment of each resource |
| **S3** | 16.2.4 | Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events. | Yes | Yes | IaC | At deployment |
| **S4** | 16.3.1 | Centralize, to the extent possible, audit log collection and retention across enterprise assets. | Yes | Yes | IaC | At deployment |
| **S5** | 16.3.2 | Retain audit logs across enterprise assets for a minimum of 90 days. | Yes | Yes | IaC | At deployment |
| **S6** | 16.3.3 | Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis. | Yes | No | Governance | Operational – review weekly |
| **S7** | 16.3.4 | Continuously monitor inbound and outbound network traffic to identify unusual activity or trends that could indicate intrusion and/or compromise of data. | Yes | No | Sentinel | Operational – review and respond to Sentinel alerts frequently |

Table 4: Security checklist summary

# NSG

The only Azure Policy required is already in place to audit NSGs being applied to subnets:

|  |  |
| --- | --- |
| Policy Name | Scopes |
| Audit subnets without Network Security Group | Landing Zones Management Group  Identity Management Group |

Table 8: Azure Policies

<https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics>

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

The following Microsoft Security Benchmark Controls are applicable[[5]](#footnote-6):

* NS-1: Establish network segmentation boundaries.
* LT-4: Enable logging for security investigation.

Beyond this, the following table outlines applicable Department of Health Controls.

### Azure Policy Security Checklist

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | DH Ref. | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **S1** | 12.1.2 | Establish and maintain a secure configuration process for network devices. | Yes | Yes | IaC | At deployment |
| **S4** | 20.1.2 | Establish, maintain and manage a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum. Ensure explicit “deny all” is used on systems to prevent unauthorised outbound connections to the internet. | Yes | Yes | IaC | At deployment |
| **S6** | 21.2.1 | Perform traffic filtering between network segments, where appropriate - the sensitivity of data needs to be taken into consideration. | Yes | Yes | IaC | At deployment |
| **S7** | 21.2.2 | Collect network traffic flow logs and/or network traffic to review and alert upon from network devices. | Yes | Yes | IaC | At deployment |
| **S8** | 24.2.3 | Maintain separate environments for production and non-production systems. | Yes | Yes | IaC | At deployment |

Table 6: Security checklist summary

# Private Endpoint and Private DNS

There are no Azure Policies required for Private Endpoints or Azure Private DNS.

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

The following Microsoft Security Benchmark controls are:

* NS-1: Establish network segmentation boundaries
* NS-2: Secure cloud services with network controls
* LT-1: Enable threat detection capabilities
* LT-4: Enable logging for security investigation

There are no Department of Health controls above and beyond the Microsoft Benchmark.

# Route Table

There are no Azure Policies relating to Route Tables that must be applied.

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

### Azure Policy Security Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **S1** | Establish, maintain and manage a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum. Ensure explicit “deny all” is used on systems to prevent unauthorised outbound connections to the internet. | Yes | Yes | IaC | At Deployment |

Table 3: Security Checklist Summary

# RSV and Backup Service

There following built-in policies should be leveraged to automate backups being enabled on VMs:

|  |  |
| --- | --- |
| Policy Name | Scope |
| Configure backup on VMs with a given tag to an existing recovery services vault in the same location | av management group (under Root) |
| Configure backup on VMs without a given tag to an existing recovery services vault in the same location | av management group (under Root) |

Table 8: Azure Policies

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

The following Microsoft Security Benchmark Controls are relevant:

* NS-2 Secure cloud services with network controls.
* IM-3 Manage application identities securely and automatically.
* DP-2 Monitor anomalies and threats targeting sensitive data.
* BR-1 Ensure regular automated backups.
* BR-2 Protect backup and recovery data.
* BR-3 Monitor backups.
* BR-4 Regularly test backup.

### Azure Policy Security Checklist

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | DH Ref. | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **S1** | 5.1.1 | Backups of important data, software and configuration settings are performed and retained with a frequency and retention timeframe in accordance with business continuity requirements. | Yes | Yes | IaC | At deployment |
| **S2** | 5.1.2 | Restoration of important data, software, and configuration settings from backups to a common point of time is tested as part of disaster recovery exercises. | Yes | No | Governance | Operational – every 6 months |
| **S3** | 5.1.3 | Unprivileged accounts cannot access backups belonging to other accounts. | Yes | No | Governance, IaC | Individual vaults deployed per application with RBAC assignments |
| **S4** | 5.1.4 | Unprivileged accounts are prevented from modifying and deleting backups. | Yes | No | Governance | Individual vaults deployed per application with RBAC assignments |
| **S5** | 5.2.1 | Unprivileged accounts, and privileged accounts (excluding backup administrators), can only access their own backups. | Yes | No | Governance | Individual vaults deployed per application with RBAC assignments |
| **S6** | 5.2.2 | Unprivileged accounts, and privileged accounts (excluding backup administrators), are prevented from modifying or deleting backups | Yes | No | Governance | Individual vaults deployed per application with RBAC assignments |
| **S7** | 5.3.1 | Unprivileged accounts, and privileged accounts (excluding backup administrators), can’t access backups. | Yes | No | Governance | Individual vaults deployed per application with RBAC assignments |
| **S8** | 5.3.2 | Unprivileged accounts, and privileged accounts (excluding backup break glass accounts), are prevented from modifying or deleting backups. | Yes | No | Governance | Individual vaults deployed per application with RBAC assignments |
| **S10** | 19.1.1 | Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | Yes | No | Governance | Operational – every 6 months |
| **S11** | 16.3.4 | Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets. | Yes | No | Governance | Operational – quarterly |
| **S12** | 19.2.2 | Maintain a physically separate recovery site that enables ready restoration of key systems in the event that their availability is lost. | Yes | Yes | IaC | At deployment |
| **S13** | 19.3.1 | Maintain sufficient isolation of its recovery service / media, such that a cyber incident on its main network couldn’t impact the recovery service / media. | Yes | Yes | IaC | At deployment |
| **S14** | 19.3.2 | Establish and maintain an isolated instance of recovery data. Example implementations include version controlling backup destinations through offline, cloud, or off-site systems or services. | Yes | Yes | IaC | At deployment |

Table 5: Security checklist summary

# Service Bus

There are no Azure Policies required for this service.

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

The following Microsoft Security Benchmark Controls are applicable:

* NS-1: Establish network segmentation boundaries
* NS-2: Secure cloud services with network controls
* IM-1: Use centralized identity and authentication system
* IM-3: Manage application identities securely and automatically
* DP-3: Encrypt sensitive data in transit
* DP-4: Enable data at rest encryption by default
* LT-4: Enable logging for security investigation

# Storage Account and Blob

There are no additional Azure policies required.

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

The following Microsoft Security Benchmark controls are applicable:

* NS-2: Secure cloud services with network controls
* IM-1: Use centralized identity and authentication system
* IM-3: Manage application identities securely and automatically
* IM-8: Restrict the exposure of credential and secrets
* DP-1: Discover, classify, and label sensitive data
* DP-2: Monitor anomalies and threats targeting sensitive data
* DP-3: Encrypt sensitive data in transit
* DP-4: Enable data at rest encryption by default
* DP-6: Use a secure key management process
* LT-4: Enable logging for security investigation
* BR-1: Ensure regular automated backups

# Traffic Manager

There are no specific Azure Policies required that relate to Azure Traffic Manager.

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft security best practices and the Department of Health controls.

The relevant Microsoft Security Controls incl

* LT-4: Enable logging for security investigation

# Virtual machines and Managed Disks

The following built-in policy will be leveraged with the following restrictions applied:

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy Name** | **Scope** | **Restricted Families** | **Allowed Families** |
| Allowed Virtual Machine SKUs | Av Prod | A Series  B Series  B Series v2  F Series v2  D Series v2  F Series  L Series  M Series | D-Series v5  D-Series v4  D-Series v3  E Series v4  E Series v5 |
| Allowed Virtual Machine SKUs | Av Non-Prod | As above but excluding B-Series as these are suitable for Non-Production. | B-Series  B-Series v2  D-Series v3  D-Series v4  D-Series v5  E Series v4  E Series v5 |

**Table 6: Azure Policies**

The above machines have been restricted based on previous recommendations and quote limitations. They are non-standard sizes or perform functions that can be achieved with other families.

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

### Azure Policy Security Checklist

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | DH Ref. | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **S1** | 2.1.1 | The execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets is prevented on workstations from within standard user profiles and temporary folders used by the operating system, web browsers and email clients. | Yes | No | Cylance | N/A to Azure for Endpoint Management  Operational – to be reviewed quarterly |
| **S2** | 2.1.2 | Application control is implemented on workstations and internet-facing servers to restrict the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set. | Yes | No | Cylance | N/A to Azure for Endpoint Management  Operational – to be reviewed quarterly |
| **S3** | 2.1.3 | Allowed and blocked executions on workstations and internet-facing servers are logged. | Yes | No | Cylance | N/A to Azure for Endpoint Management  Operational – to be reviewed quarterly |
| **S4** | 2.2.1 | Application control is implemented on workstations and servers to restrict the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications, control panel applets and drivers to an organisation-approved set. | Yes | No | Cylance | N/A to Azure for Endpoint Management  Operational – to be reviewed quarterly |
| **S5** | 2.2.2 | Microsoft’s ‘recommended block rules’ are implemented. | Yes | No | Cylance | N/A to Azure for Endpoint Management  At deployment |
| **S6** | 2.2.3 | Microsoft’s ‘recommended driver block rules’ are implemented. | Yes | No | Cylance | N/A to Azure for Endpoint Management  At deployment |
| **S7** | 2.2.4 | Application control rulesets are validated on an annual or more frequent basis. | Yes | No | Governance | N/A to Azure for Endpoint Management  Operational – to be reviewed quarterly |
| **S8** | 2.2.5 | Allowed and blocked executions on workstations and servers are centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected. | Yes | No | Sentinel | N/A to Azure for Endpoint Management  Operational - daily |
| **S9** | 3.2.4 | Administrative activities are conducted through jump servers. | Yes | Yes | Already deployed - Bastion | Operational |
| **S10** | 3.3.3 | Just-in-time administration is used for administering systems and applications. | Yes | Yes | IaC | At deployment |
| **S11** | 3.2.5 | Credentials for local administrator accounts and service accounts are long, unique, unpredictable and managed. | Yes | No | Governance, GPO | N/A to Azure for Endpoint Management  Operational - quarterly |
| **S12** | 3.3.4 | Windows Defender Credential Guard and Windows Defender Remote Credential Guard are enabled. | Yes | No | GPO | N/A to Azure for Endpoint Management |
| **S13** | 4.1.1 | Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. | Yes | Yes | IaC – Update Manager  Governance | At deployment  Operational for Zero Day exploits |
| **S14** | 4.1.2 | Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within one month of release. | Yes | Yes | IaC – Update Manager  Governance | At deployment |
| **S15** | 4.1.3 | A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services. | Yes | Yes | Tenable | N/A to Azure for Endpoint Management  Operational |
| **S16** | 4.1.4 | A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in other applications. | Yes | Yes | Tenable | N/A to Azure for Endpoint Management  Operational |
| **S17** | 4.1.5 | Operating systems that are no longer supported by vendors are replaced. | Yes | No | Governance | Operational – review quarterly |
| **S18** | 4.2.1 | Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within two weeks of release. | Yes | No | Governance | At deployment |
| **S19** | 4.2.2 | A vulnerability scanner is used at least weekly to identify missing patches or updates for security vulnerabilities in operating systems of workstations, servers and network devices. | Yes | No | Tenable | Operational - weekly |
| **S20** | 4.3.1 | Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within 48 hours if an exploit exists. | Yes | No | Governance | Operational for Zero Day exploits |
| **S21** | 4.3.2 | The latest release, or the previous release, of operating systems are used. | Yes | No | Governance | At deployment and operational |
| **S22** | 5.1.1 | Backups of important data, software and configuration settings are performed and retained with a frequency and retention timeframe in accordance with business continuity requirements. | Yes | Yes | IaC | At deployment |
| **S23** | 5.1.2 | Restoration of important data, software and configuration settings from backups to a common point of time is tested as part of disaster recovery exercises. | Yes | Yes | Governance | Operational – test quarterly |
| **S24** | 11.2.3 | Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. | Yes | Yes | IaC | At deployment |

Table 6: Security checklist summary

# Virtual Networks

The only Azure Policy required is already in place to deny the creation of public IPs.

|  |  |
| --- | --- |
| Policy Name | Scope |
| Deny the creation of public IP | av management group (under Root) |

Table 6: Azure Policies

As a security baseline, Ambulance Victoria are required to meet the Microsoft Security Benchmarks at a minimum. The relevant security controls can be found in the DH MSCB Control Mapping Gap Analysis document (version 0.5 at the time of writing this document).

The relevant network security controls from CSB are:

* NS-1: Establish network segmentation boundaries
* NS-2: Secure cloud native services with network controls
* NS-5: Deploy DDOS protection
* NS-9: Connect on-premises or cloud network privately

In addition to the above Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

### Azure Policy Security Checklist

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | DH Ref. | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **S2** | 12.3.1 | Configure trusted DNS servers on enterprise assets. Example implementations include: configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers. | Yes | Yes | IaC | At deployment |
| **S3** | 16.3.4 | Continuously monitor inbound and outbound network traffic to identify unusual activity or trends that could indicate intrusion and/or compromise of data. | Yes | Yes | IaC | Operational - Daily |
| **S4** | 20.1.2 | Establish, maintain and manage a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum. Ensure explicit “deny all” is used on systems to prevent unauthorised outbound connections to the internet. | Yes | No - to be defined in NSG Core Service Design | IaC for NSGs | At deployment |
| **S5** | 20.1.3 | Establish and maintain architecture diagram(s) and/or other network system documentation. | Yes | No | N/A | Operational – review overall architecture quarterly |
| **S6** | 21.2.1 | Perform traffic filtering between network segments, where appropriate - the sensitivity of data needs to be taken into consideration. | Yes | No - to be defined in NSG Core Service Design | IaC for NSGs | At deployment |
| **S7** | 21.2.2 | Collect network traffic flow logs and/or network traffic to review and alert upon from network devices. | Yes | No - to be defined in NSG Core Service Design | IaC for NSGs | At deployment |
| **S8** | 24.2.3 | Maintain separate environments for production and non-production systems. | Yes | Yes | IaC | At deployment |

Table 4: Security Checklist Summary

# Custom Policy Needed:-

All of the Azure policies needed for the above 30 Standardized Azure Core services, are either part of the Recommended Policy list as attached in the below Excel, or Azure Security benchmark v3. However, there are few policies that are not found as part of the two lists. These policies need to be created as a custom policy. These are noted in the Below excel sheet named Custom policy needed.





# Acceptance

Signature of this page by appropriately delegated representatives of ​Ambulance Victoria​ signifies acceptance of this design document.

Data 3 will commence build and implementation work once it receives a signed copy of this design document.

Signature of this page by appropriately delegated representatives of Ambulance Victoria signifies acceptance of this design document.

Logicalis will commence build and implementation work once it receives a signed copy of this design document.

|  |  |
| --- | --- |
| Project | Core Services |
| Document Version | 1.0 |

**Signed on behalf of Ambulance Victoria**

|  |  |
| --- | --- |
| Name |  |
| Position |  |
| Signature |  |
| Date signed |  |

**Signed on behalf of Data 3 Australia**

|  |  |
| --- | --- |
| Name |  |
| Position |  |
| Signature |  |
| Date signed |  |

1. https://learn.microsoft.com/en-us/azure/well-architected/ [↑](#footnote-ref-2)
2. https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/azure-monitor-security-baseline [↑](#footnote-ref-3)
3. https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/event-hubs-security-baseline [↑](#footnote-ref-4)
4. https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/key-vault-security-baseline [↑](#footnote-ref-5)
5. https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/virtual-network-security-baseline [↑](#footnote-ref-6)