**CORE SERVICE DESIGN:**

**Key Vault**

atabricks

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

|  |  |
| --- | --- |
| Document Control | |
| Title | Ambulance Victoria – Key Vault Core Service Design |
| **File Name** | Ambulance Victoria – Key Vault Core Service Design v1.0.docx |
| **Version** | 1.0 |
| **Status** | Released |
| **Release Date** | 15/12/2023 |

|  |  |  |  |
| --- | --- | --- | --- |
| Preparation |  |  |  |
| **Prepared** | Daniela Nikolic |  |  |
| **Authorised** | Dileep Pradeep |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Tracking | | | |  |
| Version | Remarks | Change Requested | Pages Affected | Release Date |
| 1.0 | Initial Release | N/A | All | 15/12/2023 |

Table of Contents

[1. Overview 5](#_Toc153524669)

[1.1 Purpose and Audience 5](#_Toc153524670)

[1.2 Scope and Key Deliverables 5](#_Toc153524671)

[1.3 Glossary and Definitions 6](#_Toc153524672)

[2. Executive Summary 7](#_Toc153524673)

[3. Resource Cost 8](#_Toc153524674)

[4. WAF and Security Control Alignment 9](#_Toc153524675)

[4.1 Reliability 9](#_Toc153524676)

[4.1.1 Overview 9](#_Toc153524677)

[4.1.2 Key Vault Reliability Checklist 9](#_Toc153524678)

[4.2 Cost Optimisation 10](#_Toc153524679)

[4.2.1 Overview 10](#_Toc153524680)

[4.2.2 Key Vault Cost Optimisation Checklist 10](#_Toc153524681)

[4.3 Operational Excellence 10](#_Toc153524682)

[4.3.1 Overview 10](#_Toc153524683)

[4.3.2 Key Vault Operational Excellence Checklist 10](#_Toc153524684)

[4.4 Performance Efficiency 11](#_Toc153524685)

[4.4.1 Overview 11](#_Toc153524686)

[4.4.2 Key Vault Performance Efficiency Checklist 11](#_Toc153524687)

[4.5 Security 12](#_Toc153524688)

[4.5.1 Overview 12](#_Toc153524689)

[4.5.2 Key Vault Security Checklist 13](#_Toc153524690)

[5. Architecture Summary 14](#_Toc153524691)

[5.1 Resource Overview 14](#_Toc153524692)

[5.2 RBAC 14](#_Toc153524693)

[5.3 Solution Diagram 15](#_Toc153524694)

[5.4 Design Decisions and Justifications 16](#_Toc153524695)

[5.4.1 Endpoint Connectivity 16](#_Toc153524696)

[5.4.2 Managed Identities 16](#_Toc153524697)

[5.4.3 Restrict Secret and Credential Exposure 16](#_Toc153524698)

[5.4.4 Encryption 17](#_Toc153524699)

[5.4.5 Secret, Key, and Certificate Lifecycle Management 17](#_Toc153524700)

[5.4.6 Logging and Monitoring 17](#_Toc153524701)

[5.4.7 Backup and Recovery 18](#_Toc153524702)

[5.4.8 Availability and Redundancy 18](#_Toc153524703)

[5.4.9 SKU Selection 18](#_Toc153524704)

[5.4.10 RBAC and Access Policies 18](#_Toc153524705)

[6. Azure Policies 19](#_Toc153524706)

[7. Configuration Templates 20](#_Toc153524707)

[7.1 Primary Platinum/Gold/Silver Key Vault 20](#_Toc153524708)

[7.2 DR Platinum/Gold/Silver Key Vault 20](#_Toc153524709)

[7.3 Non-Production or Bronze Key Vault 21](#_Toc153524710)

[7.4 Secret Rotation Automation Resources 22](#_Toc153524711)

[7.4.1 Primary Region Automation Account 22](#_Toc153524712)

[7.4.2 DR Region Automation Account 22](#_Toc153524713)

[8. Acceptance 24](#_Toc153524714)

# Overview

This document covers the baseline design for the Key Vault 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 Key Vault 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 Key Vault.

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 Key Vault 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. |
| **GA** | Generally Available |
| **SLA** | Service Level Agreement as defined by Microsoft |
| **DH** | Department of Health |
| **IaC** | Infrastructure as Code |
| **NSG** | Network Security Groups |
| **KV** | Key Vault |

Table : Glossary and definitions

# Executive Summary

This design covers the baseline standards for the Key Vault Core Service. This service has been assessed against the five pillars of WAF as well as the Department of Health Security Controls.

This section contains a summary of the major design decisions that have been made for defining the baseline of this resource as an outcome of the WAF and Security analysis detailed throughout this document.

Of the five WAF Pillars, it was found that there was no Key Vault specific service guidance. There were some Platform level recommendations to enable Alerting that have been included.

For the specific configuration items, the Platinum, Gold, and Silver Key Vaults have the same configurations as these are all generally Production that require enhanced protection. For Bronze or Non-Production workloads the main difference in configuration is a shortened soft-delete retention period (14 days as opposed to 90 days).

The secret rotation process will require an additional automation account per region, with a runbook that will automatically update secrets in the Key Vault within 30 days of their expiry.

# Resource Cost

Key Vault pricing is based on the Vault itself, as well as the operations performed within it[[2]](#footnote-3). There are two tiers: Standard and Premium.

|  |  |  |
| --- | --- | --- |
| Vault Operations | Standard SKU | Premium SKU |
| Secrets Operations | $0.046/10,000 transactions | $0.046/10,000 transactions |
| Certificate Operations | Renewals - $4.518 per renewal request  All other operations - $0.046/10,000 transactions | Renewals - $4.518 per renewal request  All other operations - $0.046/10,000 transactions |
| Managed Azure Storage account key rotation (in preview) | Free during preview.  GA price - $1.506 per renewal | Free during preview.  GA price - $1.506 per renewal |
| **Software Protected Keys** | **Standard SKU** | **Premium SKU** |
| RSA 2048-bit keys | N/A | $1.506 per key per month  +  $0.046/10,000 transactions |
| Advanced key types:  RSA 3072-bit, RSA 4096-bit, and Elliptic-Curve Cryptography (ECC) keys | N/A | First 250 keys - $7.529 per key per month |
| 251-1500 keys - $3.765 per key per month |
| 1501-4000 keys - $1.356 per key per month |
| 4001+ keys - $0.603 per key per month |
| + $0.226/10,000 transactions |
| **Key Rotation** | **Standard SKU** | **Premium SKU** |
| Automated Key Rotation | $1.506 per rotation | $1.506 per rotation |
| **Managed HSM Pools** | **Standard SKU** | **Premium SKU** |
| Standard B1 | $4.819 | $4.819 |

Table 1: Pricing Construct

# WAF and Security Control Alignment

The following are the five pillars of the Microsoft Well Architected Framework:

* [Reliability](https://learn.microsoft.com/en-us/azure/well-architected/#reliability)
* [Cost optimization](https://learn.microsoft.com/en-us/azure/well-architected/#cost-optimization)
* [Operational excellence](https://learn.microsoft.com/en-us/azure/well-architected/#operational-excellence)
* [Performance efficiency](https://learn.microsoft.com/en-us/azure/well-architected/#performance-efficiency)
* [Security](https://learn.microsoft.com/en-us/azure/well-architected/#security)

For this design, the security section will also cover the Department of Health Controls in addition with any Microsoft Security Best Practices. Each of these sections will detail relevant controls or baseline requirements for this core service that will be put in place.

## Reliability

### Overview

The term reliability refers to the availability of the system and its ability to recover from failure[[3]](#footnote-4). Resiliency strategies must be built into each element of the architecture. The pillars of reliability include:

* Design for business requirements
* Design for failure
* Observe application health
* Drive Automation

### Key Vault Reliability Checklist

There is no service specific guidance for Reliability for Azure Key Vault. This is because Azure Key Vaults are inherently Highly Available and redundant[[4]](#footnote-5). Due to the nature of the service and the sensitive content stored, there are several redundancy layers built into this service without any additional configurations required.

For Azure Regions that are paired with another region, the contents of the Key Vault are replicated within the region, and to the paired region. In this case the replication will be between Australia Southeast and Australia East. Failover to this secondary region is automatic, and failback is also automatic. No additional steps are required.

## Cost Optimisation

### Overview

The cost optimisation pillar is structured to support creating cost-effective workloads in the cloud[[5]](#footnote-6). It looks at removal of unnecessary spend and improving operational efficiency. The principles of cost optimisation revolve around:

* Choosing the correct resources
* Setting up budgets and maintaining cost constraints
* Dynamically allocate and deallocate resources
* Optimising workloads whilst aiming for scalable costs
* Continuously monitoring and cost managing

### Key Vault Cost Optimisation Checklist

There is no service specific guidance for Cost Optimisation for Azure Key Vault.

## Operational Excellence

### Overview

Operational Excellence aims to ensure that once the architecture is built, the ongoing operations are flawless. This includes repeatable and reliable deployments, automating to eliminate human error. To do this the following must be considered:

* Optimise the build and release process (including CI/CD and IaC)
* Understand Operational Health
* Test recovery and failure
* Focus on continuous improvement
* Use loosely coupled architecture

### Key Vault Operational Excellence Checklist

There is no service specific guidance for Operational Excellence for Azure Key Vault.

## Performance Efficiency

### Overview

Performance Efficiency refers to the ability of your systems and applications to meet user demands without breaking or creating a negative user experience[[6]](#footnote-7). This covers capacity and scalability:

* Design for horizontal scaling
* Run stress and performance tests
* Continuously monitor performances, particularly in Production systems

### Key Vault Performance Efficiency Checklist

There is no service specific guidance for Performance Efficiency for Azure Key Vault. Diagnostics and alerting will be created for Key Vault as per Platform-level guidance.

## Security

### Overview

Security refers to the ability of the environment to resist and manage threats.

This section covers both Microsoft Best Practices as well as relevant security controls provided by the Department of Health. With respect to the Microsoft WAF, Security is underpinned by the following[[7]](#footnote-8):

* Plan resources and how to harden them
* Automate and use least privilege
* Classify and encrypt data
* Monitor system security, plan incident response
* Identify and protect endpoints
* Protect against code-level vulnerabilities
* Model and test against potential threats

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[[8]](#footnote-9):

* 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.

### Key Vault 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 : Security checklist summary

# Architecture Summary

## Resource Overview

Azure Key Vault is an Azure native service that is used for secure storage of certificates, keys, and secrets[[9]](#footnote-10). It allows you to centralise storage of application-related secrets, and securely store secrets and keys.

## RBAC

For Azure Key Vault the following RBAC roles can be applied[[10]](#footnote-11):

|  |  |
| --- | --- |
| Role Name | Description |
| Key Vault Administrator | Perform all data plane operations on a key vault and all objects in it, including certificates, keys, and secrets. Cannot manage key vault resources or manage role assignments. Only works for key vaults that use the 'Azure role-based access control' permission model. |
| Key Vault Certificates Officer | Perform any action on the certificates of a key vault, except manage permissions. Only works for key vaults that use the 'Azure role-based access control' permission model. |
| Key Vault Crypto Officer | Perform any action on the keys of a key vault, except manage permissions. Only works for key vaults that use the 'Azure role-based access control' permission model. |
| Key Vault Crypto Service Encryption User | Read metadata of keys and perform wrap/unwrap operations. Only works for key vaults that use the 'Azure role-based access control' permission model. |
| Key Vault Crypto User | Perform cryptographic operations using keys. Only works for key vaults that use the 'Azure role-based access control' permission model. |
| Key Vault Reader | Read metadata of key vaults and its certificates, keys, and secrets. Cannot read sensitive values such as secret contents or key material. Only works for key vaults that use the 'Azure role-based access control' permission model. |
| Key Vault Secrets Officer | Perform any action on the secrets of a key vault, except manage permissions. Only works for key vaults that use the 'Azure role-based access control' permission model. |
| Key Vault Secrets User | Read secret contents including secret portion of a certificate with private key. Only works for key vaults that use the 'Azure role-based access control' permission model. |

Table : RBAC roles relevant for this core service

## Solution Diagram

Figure : Key Vault with and without secret rotation

## Design Decisions and Justifications

This section covers the design decisions and justifications that reflect the findings of the WAF and Security alignment. This will form the baseline requirements for the Key Vault core service and will be captured in the accompanying Configuration Template with a set of pre-approved deployment settings for this resource. Any changes, modifications or removals to the pre-approved deployments must have specific approval from the Cloud Governance Forum prior to deployment.

### Endpoint Connectivity

**Design Reference:** Microsoft Security Benchmark [NS-1, NS-2](#_Overview)

**Design Decision:** Use Private Endpoints for connectivity as a priority. If this cannot be achieved for any architectural reason, then Service Endpoints should be used as an alternative. Additionally, Azure Policy should be used to audit the configuration of Key Vaults from a connectivity perspective. Public Access should always be disabled.

**Design Justification:** Private endpoints provide the most secure form of connectivity and should be used as a priority for Key Vault connectivity. If in any case an application is unable to use this, only then should Service Endpoints be used. Public access should never be allowed on Key Vault resources, and Azure Policy will be used to audit this.

### Managed Identities

**Design Reference:** Microsoft Security Benchmark [IM-3](#_Overview)

**Design Decision:** Managed Identities will be used instead of Service Principals where possible for secure authentication. As such, System-Assigned Managed Identities will be enabled.

**Design Justification:** With Managed Identities, Azure can natively manage the security of this object. Managed Identity credentials are fully managed by Azure, and frequently rotated by the platform which avoids hardcoding in source-code or files. It is more secure than manually managing Service Principal credentials and removes administrative burden from Ambulance Victoria.

### Restrict Secret and Credential Exposure

**Design Reference:** Microsoft Security Benchmark [IM-8](#_Overview)

**Design Decision:** Use Azure Key Vault as the native secret and credential storage resource

**Design Justification:** To avoid insecure storage of credentials (such as hardcoding in code or in configuration files), Azure Key Vault will be used as the primary credential storage location for Cloud resources.

### Encryption

**Design Reference:** Microsoft Security Benchmark [DP-3, DP-4](#_Overview)

**Design Decision**: Azure Key Vault has native encryption capabilities. No additional configuration required after deployment.

**Design Justification**: Azure Key Vault will automatically enable encryption as a default deployment[[11]](#footnote-12). The Azure Platform also encrypts data in transit when it is moving between Azure services, so no additional work is required to meet this control after deployment[[12]](#footnote-13).

### Secret, Key, and Certificate Lifecycle Management

**Design Reference:** Microsoft Security Benchmark [DP-6](#_Overview), DP-7

**Design Decision:** Configure automated rotation of Keys (native to the Key Vault) and create automations for the rotation of secrets (this cannot be done natively to the Key Vault). Certificates cannot be automatically generated and uploaded, so an alert will be configured to remind users to renew these. Additionally, Azure Policies will be used to track keys and secrets expiry dates. The rotation of secrets requires additional resources but will be implemented.

**Design Justification:** To reduce administrative overhead, as much of the renewal processes for keys, secrets, and certificates will be automated. Alerts will also be configured so that the relevant teams are aware that an action is required. Each time a new Key Vault is created that requires secrets, such as that for Service Principals, an automation involving an Automation Account with a Managed Identity must be created to ensure that renewals can take place automatically.

### Logging and Monitoring

**Design Reference:** Microsoft Security Benchmark [LT-1,LT-4](#_Overview)

**Design Decision:** Microsoft Defender for Key Vault will be enabled. Diagnostics logs will be sent to central log analytics workspace.Alerts will be created for create, delete, update of Key Vaults to catch any changes that could be malicious.

**Design Justification:** Given the nature of this resource containing highly sensitive information it is imperative to have full monitoring and logging enabled. Microsoft Defender for Key Vault will be enabled on all subscriptions as they are created. allLogs and allMetrics will be sent to the central log analytics workspace for that region.For additional security, alerts for Audit log updates (such as creating, deleting, or modifying) for Key Vault will be configured.

### Backup and Recovery

**Design Reference:** Microsoft Security Benchmark [BR-1](#_Overview)

**Design Decision:** Soft-delete and purge protection will be enabled. The native backup functionality will not be used unless a critical business need requires it.

**Design Justification:** Enabled soft-delete and purge protection meet this security control and protect against malicious attempts at deletions. The native backup functionality in Azure Key Vault does not back up the entire vault and can only backup individual objects at a time. It is not recommended to use this feature unless there is a highly critical business need for it[[13]](#footnote-14). Purge protection should be disabled for Dev and Test workloads so that vault objects can be purged manually as they are being developed. The same can be considered for soft-delete.

### Availability and Redundancy

**Design Reference:** Table 6 – [S1](#_Key_Vault_Security)

**Design Decision:** No action is required for High Availability.

**Design Justification:** Azure Key Vault automatically copies data to the paired region (Australia East if using Australia Southeast as the Primary and vice versa). No action is required to enable this.

### SKU Selection

**Design Reference:** Cost Optimisation Section

**Design Decision:** The Standard SKU will be used unless there is a requirement for the features of Premium (HSM and enhanced cryptography).

**Design Justification:** The Standard SKU is suitable for general use cases for most applications. If there is a requirement for enhanced features, then the Premium tier can be used.

### RBAC and Access Policies

**Design Reference:** N/A

**Design Decision:** Use RBAC for access management.

**Design Justification:** Access Policies are a legacy form of managing access to Key Vaults and are being deprecated. As such only RBAC will be used, in alignment with all other Azure resources.

# Azure Policies

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 : 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 : Additional Azure Policies

# Configuration Templates

## Primary Platinum/Gold/Silver Key Vault

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Configuration Item | Configuration Details | | | |
| Subscription | AV ALZ [Subscription Name] | | | |
| Name | kv-[env]-ause-[appname]-[workload]-01 | | | |
| SKU | Standard | | | |
| Soft-delete | Enabled | | | |
| Days to retain deleted vaults | 90 | | | |
| Purge protection | Enabled | | | |
| Enabled for VM Access | True | | | |
| Enabled for ARM Template Deployment | True | | | |
| Enabled for Azure Disk Encryption | True | | | |
| Permission Model | RBAC | | | |
| Public Access | Disabled | | | |
| Private Endpoint | Enabled | | | |
| Firewall Rules | If Private Endpoint cannot be supported whitelist selected allowed networks | | | |
| Firewall Rules | **Virtual Network/IP** | **Subnet** | |
|  |  | |
|  |  | |
|  |  | |
| Encryption | Enabled (encryption key managed by Microsoft) | | | |
| Alerts | Create, Update, or Delete Key Vault | | | |
| Logging | allLogs and allMetrics to be sent to law-prd-ause-mgmt-01 | | | |
| Defender for Key Vault | Enabled | | | |
| Key Rotation Policy | Options | | Generate | |
|  | Name | | kvrp-[env]-ause-[appname]-[workload]-01 | |
|  | Key Type | | RSA | |
|  | RSA Size | | 2048 | |
|  | Expiration | | 90 days | |

## DR Platinum/Gold/Silver Key Vault

|  |  |  |  |
| --- | --- | --- | --- |
| Configuration Item | Configuration Details | | |
| Subscription | AV ALZ [Subscription Name] | | |
| Name | kv-dr-auea-[appname]-[workload]-01 | | |
| SKU | Standard | | |
| Soft-delete | Enabled | | |
| Days to retain deleted vaults | 90 | | |
| Purge protection | Enabled | | |
| Enabled for VM Access | True | | |
| Enabled for ARM Template Deployment | True | | |
| Enabled for Azure Disk Encryption | True | | |
| Permission Model | RBAC | | |
| Public Access | Disabled | | |
| Private Endpoint | Enabled | | |
| Firewall Rules | If Private Endpoint cannot be supported whitelist selected allowed networks | | |
| Firewall Rules | **Virtual Network/IP** |
|  |
|  |
|  |
| Encryption | Enabled (encryption key managed by Microsoft) | | |
| Alerts | Create, Update, or Delete Key Vault | | |
| Logging | allLogs and allMetrics to be sent to law-prd-auea-mgmt-01 | | |
| Defender for Key Vault | Enabled | | |
| Key Rotation Policy | Options | | Generate |
| Name | | kvrp-[env]-auea-[appname]-[workload]-01 |
| Key Type | | RSA |
| RSA Size | | 2048 |
| Expiration | | 90 days |

## Non-Production or Bronze Key Vault

|  |  |  |  |
| --- | --- | --- | --- |
| Configuration Item | Configuration Details | | |
| Subscription | AV ALZ [Subscription Name] | | |
| Name | kv-[env]-ause-[appname]-[workload]-01 | | |
| SKU | Standard | | |
| Soft-delete | Enabled | | |
| Days to retain deleted vaults | 14 | | |
| Purge protection | Disabled | | |
| Enabled for VM Access | True | | |
| Enabled for ARM Template Deployment | True | | |
| Enabled for Azure Disk Encryption | True | | |
| Permission Model | RBAC | | |
| Public Access | Disabled | | |
| Private Endpoint | Enabled | | |
| Firewall Rules | If Private Endpoint cannot be supported whitelist selected allowed networks | | |
| Firewall Rules | **Virtual Network/IP** |
|  |
|  |
|  |
| Encryption | Enabled (encryption key managed by Microsoft) | | |
| Alerts | Create, Update, or Delete Key Vault | | |
| Logging | allLogs and allMetrics to be sent to law-prd-ause-mgmt-01 | | |
| Defender for Key Vault | Enabled | | |
| Key Rotation Policy | Options | | Generate |
| Name | | kvrp-[env]-ause-[appname]-[workload]-01 |
| Key Type | | RSA |
| RSA Size | | 2048 |
| Expiration | | 180 days |

## Secret Rotation Automation Resources

### Primary Region Automation Account

|  |  |
| --- | --- |
| Configuration Item | Configuration Details |
| Subscription | AV ALZ Management |
| Name | aa-prd-ause-kvrotation-mgmt-01 |
| Managed Identity | System Assigned |
| Networking | Private Access |
| Private Endpoint | pe-aa-prd-ause-kvrotation-mgmt-01 |
| Target Sub-resource | DSCandHybridWorker |
| Virtual Network | vnet-prd-ause-mgmt-01 |
| Subnet | (New) [sn-prd-ause-privatelink-01](https://portal.azure.com/) |
| Private DNS Zone | Privatelink.azure-automation.net |
| Runbook | SecretRotationRunbook |

### DR Region Automation Account

|  |  |
| --- | --- |
| Configuration Item | Configuration Details |
| Subscription | AV ALZ Management |
| Name | aa-prd-auea-kvrotation-mgmt-01 |
| Managed Identity | System Assigned |
| Networking | Private Access |
| Private Endpoint | pe-aa-prd-auea-kvrotation-mgmt-01 |
| Target Sub-resource | DSCandHybridWorker |
| Virtual Network | vnet-prd-ause-mgmt-01 |
| Subnet | (New) [sn-prd-auea-privatelink-01](https://portal.azure.com/) |
| Private DNS Zone | Privatelink.azure-automation.net |
| Runbook | SecretRotationRunbook |

The details of the code underlying the Runbook will not be detailed here. They will be provided as an additional item, like the IaC scripts, tested and submitted separately for Ambulance Victoria’s approval.

# Acceptance

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.

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 | Dan Howarth |
| Position |  |
| Signature |  |
| Date signed |  |

**Signed on behalf of Logicalis Australia**

|  |  |
| --- | --- |
| Name | Daniela Nikolic |
| Position | Senior Cloud Engineer |
| Signature |  |
| Date signed |  |

1. https://learn.microsoft.com/en-us/azure/well-architected/ [↑](#footnote-ref-2)
2. https://azure.microsoft.com/en-us/pricing/details/key-vault/ [↑](#footnote-ref-3)
3. https://learn.microsoft.com/en-us/azure/well-architected/resiliency/overview [↑](#footnote-ref-4)
4. https://learn.microsoft.com/en-us/azure/key-vault/general/disaster-recovery-guidance [↑](#footnote-ref-5)
5. https://learn.microsoft.com/en-us/azure/well-architected/cost/overview [↑](#footnote-ref-6)
6. https://learn.microsoft.com/en-us/azure/well-architected/scalability/overview [↑](#footnote-ref-7)
7. https://learn.microsoft.com/en-us/azure/well-architected/security/security-principles [↑](#footnote-ref-8)
8. https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/key-vault-security-baseline [↑](#footnote-ref-9)
9. https://learn.microsoft.com/en-us/azure/key-vault/general/overview [↑](#footnote-ref-10)
10. https://learn.microsoft.com/en-us/azure/key-vault/general/rbac-guide?tabs=azure-cli [↑](#footnote-ref-11)
11. https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/key-vault-security-baseline [↑](#footnote-ref-12)
12. https://learn.microsoft.com/en-us/azure/security/fundamentals/double-encryption#data-in-transit [↑](#footnote-ref-13)
13. https://github.com/MicrosoftDocs/azure-docs/blob/main/articles/key-vault/general/backup.md [↑](#footnote-ref-14)