Security Baseline sample policy statements

02/11/2019 • 4 minutes to read • Contributors

In this article

Individual cloud policy statements are guidelines for addressing specific risks identified during your risk assessment process. These statements should provide a concise summary of risks and plans to deal with them. Each statement definition should include these pieces of information:

- **Technical risk:** A summary of the risk this policy will address.
- **Policy statement:** A clear summary explanation of the policy requirements.
- **Technical options:** Actionable recommendations, specifications, or other guidance that IT teams and developers can use when implementing the policy.

The following sample policy statements address common security-related business risks. These statements are examples you can reference when drafting policy statements to address your organization's needs. These examples are not meant to be proscriptive, and there are potentially several policy options for dealing with each identified risk. Work closely with business, security, and IT teams to identify the best policies for your unique set of risks.

Asset classification

Technical risk: Assets that are not correctly identified as mission-critical or involving sensitive data may not receive sufficient protections, leading to potential data leaks or business disruptions.

Policy statement: All deployed assets must be categorized by criticality and data classification. Classifications must be reviewed by the Cloud Governance team and the application owner before deployment to the cloud.

Potential design option: Establish resource tagging standards and ensure IT staff apply them consistently to any deployed resources using Azure resource tags.

Data encryption

Technical risk: There is a risk of protected data being exposed during storage.

Policy statement: All protected data must be encrypted when at rest.

Potential design option: See the Azure encryption overview article for a discussion of how data at rest encryption is performed on the Azure platform.

Network isolation

Technical risk: Connectivity between networks and subnets within networks introduces potential vulnerabilities that can result in data leaks or disruption of mission-critical services.

Policy statement: Network subnets containing protected data must be isolated from any other subnets. Network traffic between protected data subnets is to be audited regularly.

Potential design option: In Azure, network and subnet isolation is managed through Azure Virtual Networks.

Secure external access

Technical risk: Allowing access to workloads from the public internet introduces a risk of intrusion resulting in unauthorized data exposure or business disruption.

Policy statement: No subnet containing protected data can be directly accessed over public internet or across datacenters. Access to those subnets must be routed through intermediate subnet works. All access into those subnets must come through a firewall solution capable of performing packet scanning and blocking functions.

Potential design option: In Azure, secure public endpoints by deploying a DMZ between the public internet and your cloud-based network.

DDoS protection

Technical risk: Distributed denial of service (DDoS) attacks can result in a business interruption.

Policy statement: Deploy automated DDoS mitigation mechanisms to all publicly accessible network endpoints.

Potential design option: Use Azure DDoS Protection to minimize disruptions caused by DDoS attacks.

Secure on-premises connectivity

Technical risk: Unencrypted traffic between your cloud network and on-premises over the public internet is vulnerable to interception, introducing the risk of data exposure.

Policy statement: All connections between the on-premises and cloud networks must take place either through a secure encrypted VPN connection or a dedicated private WAN link.

Potential design option: In Azure, use ExpressRoute or Azure VPN to establish private connections between your on-premises and cloud networks.

Network monitoring and enforcement

Technical risk: Changes to network configuration can lead to new vulnerabilities and data exposure risks.

Policy statement: Governance tooling must audit and enforce network configuration requirements defined by the Security Baseline team.

Potential design option: In Azure, network activity can be monitored using Azure Network Watcher, and Azure Security Center can help identify security vulnerabilities. Azure Policy allows you to restrict network resources and resource configuration policy according to limits defined by the security team.

Security review

Technical risk: Over time, new security threats and attack types emerge, increasing the risk of exposure or disruption of your cloud resources.

Policy statement: Trends and potential exploits that could affect cloud deployments should be reviewed regularly by the security team to provide updates to Security Baseline tooling used in the cloud.

Potential design option: Establish a regular security review meeting that includes relevant IT and governance team members. Review existing security data and metrics to establish gaps in current policy and Security Baseline tooling, and update policy to remediate any new risks.

Next steps

Use the samples mentioned in this article as a starting point to develop policies that address specific security risks that align with your cloud adoption plans.

To begin developing your own custom policy statements related to Security Baseline, download the Security Baseline template.

To accelerate adoption of this discipline, choose the actionable governance journey that most closely aligns with your environment. Then modify the design to incorporate your specific corporate policy decisions.

Actionable governance journeys