What is the Azure/SQL policy for Data Security?

Use firewall rules to restrict database access

Microsoft Azure SQL Database provides a relational database service for Azure and other internet-based applications. To provide access security, SQL Database controls access with:

- Firewall rules that limit connectivity by IP address.
- Authentication mechanisms that require users to prove their identity.
- Authorization mechanisms that limit users to specific actions and data.

Firewalls prevent all access to your database server until you specify which computers have permission. The firewall grants access to databases based on the originating IP address of each request. Data protection Azure provides customers with strong data security, both by default and as customer options.

Data segregation

Azure is a multi-tenant service, which means that multiple customer deployments and VMs are stored on the same physical hardware. Azure uses logical isolation to segregate each customer's data from the data of others. Segregation provides the scale and economic benefits of multi-tenant services while rigorously preventing customers from accessing one another's data.

At-rest data protection

Customers are responsible for ensuring that data stored in Azure is encrypted in accordance with their standards. Azure offers a wide range of encryption capabilities, giving customers the flexibility to choose the solution that best meets their needs. Azure Key Vault helps customers easily maintain control of keys that are used by cloud applications and services to encrypt data. Azure Disk Encryption enables customers to encrypt VMs. Azure Storage Service Encryption makes it possible to encrypt all data that is placed into a customer's storage account.

In-transit data protection

Customers can enable encryption for traffic between their own VMs and end users. Azure protects data in transit to or from outside components and data in transit internally, such as between two virtual networks. Azure uses the DocuSign Envelope ID: B8F12680-F0E9-4996-BEDF-EF00D81F11B6 industry-standard Transport Layer Security (TLS) 1.2 or later protocol with 2,048-bit RSA/SHA256 encryption keys, as recommended by CESG/NCSC, to encrypt communications between:

- The customer and the cloud.
- Internally between Azure systems and datacenters.

Encryption

Encryption of data in storage and in transit can be deployed by customers as a best practice for ensuring confidentiality and integrity of data. It is straightforward for customers to configure their Azure cloud services to use SSL to protect communications from the internet and even between their Azure-hosted VMs.

Data redundancy

Microsoft helps ensure that data is protected if there is a cyberattack or physical damage to a datacenter. Customers may opt for:

- In-country/in-region storage for compliance or latency considerations.
- Out-of-country/out-of-region storage for security or disaster recovery purposes.

Data can be replicated within a selected geographic area for redundancy but cannot be transmitted outside it. Customers have multiple options for replicating data, including the number of copies and the number and location of replication datacenters.

When you create your storage account, select one of the following replication options:

- **Locally redundant storage (LRS):** Locally redundant storage maintains three copies of your data. LRS is replicated three times within a single facility in a single region. LRS protects your data from normal hardware failures, but not from a failure of a single facility.

- **Zone-redundant storage (ZRS):** Zone-redundant storage maintains three copies of your data. ZRS is replicated three times across two to three facilities to provide higher durability than LRS. Replication occurs within a single region or across two regions. ZRS helps ensure that your data is durable within a single region.

- **Geo-redundant storage (GRS):** Geo-redundant storage is enabled for your storage account by default when you create it. GRS maintains six copies of your data. With GRS, your data is replicated three times within the primary region. Your data is also replicated three times in a secondary region hundreds of miles away from the primary region, providing the highest level of durability. In the event of a failure at the primary region, Azure Storage fails over to the secondary region. GRS helps ensure that your data is durable in two separate regions.

Data destruction

When customers delete data or leave Azure, Microsoft follows strict standards for overwriting storage resources before their reuse, as well as the physical DocuSign Envelope ID: B8F12680-F0E9-4996-BEDF-EF00D81F11B6 destruction of decommissioned hardware. Microsoft executes a complete deletion of data on customer request and on contract termination.

Protect your data by using encryption

To help protect data in the cloud, you need to account for the possible states in which your data can occur, and what controls are available for that state. Best practices for Azure data security and encryption relate to the following data states:

- At rest: This includes all information storage objects, containers, and types that exist statically on physical media, whether magnetic or optical disk.

- Apply disk encryption to help safeguard your data.

- In transit: When data is being transferred between components, locations, or programs, it's in transit. Examples are transfer over the network, across a service bus (from on-premises to cloud and vice-versa, including hybrid connections such as ExpressRoute), or during an input/output process.

We generally recommend that you always use SSL/TLS protocols to exchange data across different locations.

Encryption Safeguards

In addition, Microsoft uses encryption to safeguard customer data and help you maintain control over it. When data moves over a network—between user devices and Microsoft datacenters or within datacenters themselves—Microsoft products and services use industry-standard secure transport protocols. To help protect data at rest, Microsoft offers a range of built-in encryption capabilities.

Most Microsoft business cloud services are multitenant services, meaning that your data, deployments, and virtual machines may be stored on the same physical hardware as that of other customers. Microsoft uses logical isolation to segregate storage and processing for different customers through specialised technology engineered to help ensure that your customer data is not combined with anyone else's.

Business cloud services with audited certifications such as ISO 27001 are regularly verified by Microsoft and accredited audit firms, which perform sample audits to attest that access is only for legitimate business purposes.