Centero Customer Portal Security Controls

Last Modified

Network

Network connections to Customer Portal is protected by Azure Front Door service. All connections to Customer Portal use HTTPS (minimum of TLS 1.2).

Authentication

Access to Customer Portal is restricted by Azure Active Directory authentication and authorization is based on roles. Customer Portal is Microsoft Azure Active Directory application so Customer can define additional authentication requirements for the application (like conditional access and MFA). Roles each user has in Customer Portal can be managed by Customer admin users in Customer Portal.

Logging

Audit logging for actions performed in Customer Portal are available for customers only trough separate service requests.

Platform

Customer Portal is running on Microsoft Azure platform. Location of the services in Microsoft Azure is in Europe either North Europe or West Europe datacenters.

Physical Security

As Customer Portal is running on Microsoft Azure platform the description how physical security is handled can be found from Microsoft documentation: Physical security of Azure datacenters - Microsoft Azure | Microsoft Docs

Compute Security

Access to Customer Portal service related Azure resources is restricted for specific Centero personnel using Azure Security Control and limited only to persons responsible for maintaining the Customer Portal. Microsoft Defender for Cloud is used to protect Azure resources. Access from Internet is restricted only to HTTPS based Centero Portal. Access to databases is restricted only to selected Centero public IP addresses.

Data security (Data-at-rest)

Data stored in Azure for Centero Portal is encrypted at rest. This includes Azure storage and databases. Encryption keys are managed by Azure platform.

Network security (Data-at-transit)

All data for Centero Portal coming in to Azure and going out from Azure is always SSL (minimum TLS 1.2) encrypted.

Availability and monitoring

Custom ased on M cr soft Azure s vice availability. Recovery from technical platform Backups for Centero Portal content is taken by Azure Recovery Services with sh strategy. Customer Portal is monitored internally on Azure using Azure Monitor Internet. A ure Alerts service is used to open internal service tickets for issues and A monitoring operations team of the Customer Portal.