CERTUS AUTOMATION

CERTUS Automation Security Policy

Version 2.0, Release date 27-10-2021

Data Protection & Encryption

All data within the CERTUS solution is located within the customer network and behind the customer firewall.
Data only transits within the customer owned and controlled network environment.
CERTUS services are using certified monitoring tooling to safeguard the availability and/or capacity of data.
Automatic alerting to the CERTUS service team ensures proper functionality.
Advice or action is taken by the service team depending of the contractual obligations.

Identity & Access Management

We are currently using 2FA (Two-Factor Authentication) for our remote access to customer installations and deploying 2FA for Office 365 within CERTUS.
Certus is preventing the use of soft tokens in favor of Google & Microsoft Authenticators, for example.
Within Certus, 1Password is used for securely storing passwords and the use of this is mandatory.
We also strongly advise (sometimes enforce when needed) use of named accounts for support engineers at customer sites.

Asset Identification & Inventory Management

CERTUS installs all equipment in the customer network.
All ip-related equipment is secured based on customer defined criticality levels and security rules.
Data retention in many cases is aligned by customer requirements e.g. the time a picture needs to be available to the terminal.
Internally, CERTUS complies with the GDPR rules and regulations in regard to data retention

Asset Change Control & Maintenance

CERTUS remote access is directed by our customer's IT department i.e. connection management, authentication management and access security management.
CERTUS conforms to the security rules in regard to the used connection tools and technologies.
All access to customer sites are controlled and dispatched from the remote support group.
In cases where this is not possible CERTUS security rules are enforced.
This includes local IT security requirements. e.g. specific access SW, dual authentication and firewall enablement per instance.

Governance

Regulatory insurance is obtained by the certifications ISO, VCA, GDPR, ISMS.
CERTUS also has to ensure compliance to our customer specific regulations e.g. the USA data crime act and other specific local regulations.
Oversight is obtained by compliance to EEC, and non EEC compliance rules in combination with the WW compliance rules and regulations.
Any third party working on the behalf of CERTUS is required to comply to the same level CERTUS enforces.

Security Incident Response

Internal incidents are identified by the procedures in place at the IT level. External incidents are identified by customer IT departments and potentially by the CERTUS remote service team. A customer impact report will be communicated immediately via phone, email and JIRA

Security Monitoring

Our AWS and Azure tenants are monitored using Tenablo.io. Using the relevant CIS controls, we have two secure and compliant tenants.
Within Certus we are using a SIEM solution for collecting log files from all managed servers.
We are actively monitoring our environment thus preventing external intrusions.
CERTUS is using managed Fortinet next generation firewalls.

CERTUS is GDPR, ISO and equivalent WW requirements compliant.

CERTUS Port Automation B.V.
Rietlanden 3 | 3361 AN | SLIEDRECHT | The Netherlands
Tel: +31 85 0068800
support@certusautomation.com
www.certusautomation.com