SANITARY BY DESIGN
ANDERSON-NEGELE

Anderson Instrument Co., Inc.
156 Auriesville Road
Fultonville, NY 12072
518-922-5315
518-922-8997 (fax)
www.anderson-negele.com

Anderson-Negele

Paperless Process Recorder & Legendary™ Information Security Statement

July 2021

Document Number 80002/ 1.0.1 / 2021-07-27 / RF / NA

SANITARY BY DESIGN
ANDERSON-NEGELE

Anderson Instrument Co., Inc.
156 Auriesville Road
Fultonville, NY 12072
518-922-5315
518-922-8997 (fax)
www.anderson-negele.com

Overview

Anderson-Negele takes the security of Anderson-Negele's information, infrastructure, and applications seriously. We understand that confidentiality and data security are vital to our customers and their businesses. Anderson-Negele takes a multi-layered approach to ensuring customer satisfaction and trust which includes secure data centers, disaster recovery, data backups, security assessments, strong encryption, around the clock monitoring, third party assessments, and industry best practices.

Data Center Security

The Legendary™ software uses Rackspace as a data center. The infrastructure is designed, deployed, supported, and administered using industry-standard best practices in the areas including but not limited to:

- selection and use of hardware and software services
- redundancy of critical equipment
- backup, restoration, and failover capabilities
- privileged access restriction to authorized individuals
- maintenance of principle of least privilege

Threat and Vulnerability Management

A multi-layer approach is used to identify potential threats that would impair system security and availability, analyze the significance of risks associated with the identified threats and determine mitigation strategies for those risks. Threats and vulnerabilities are identified by means of:

- automated testing and scanning of software releases
- automated and manual scanning of infrastructure and underlying components; and
- input from incident management process

A risk-based approach is used to analyze and determine a remediation strategy of threats and vulnerabilities.

Intrusion Detection and Prevention

The Legendary™ infrastructure is protected by intrusion detection and intrusion prevention systems. These systems monitor traffic and action anomalous behaviors as follows:

- alerting hosting provider for further investigation and manual intervention

Anderson Instrument Co., Inc.
156 Auriesville Road
Fultonville, NY 12072
518-922-5315
518-922-8997 (fax)
www.anderson-negele.com

- automatically blocking (shunning) traffic from source addresses. Blocks may be temporary (24-hours) or permanent, depending on the history and/or reputation of the source. Activities that may trigger a shun may include attempt to scan or reconnoiter the environment, attempt to actively attack, or exploit the environment, and violate policy rules.

Incident Management

Anderson-Negele follows a formalized security incident management process to evaluate and provide timely response to security incident and event notifications. Incidents are triggered from a variety of sources including:

- Automated monitoring and alerting tools;
- Cybersecurity diligence from threat bulletins, news wires and vendor statement;
- Direct notifications from employees, customers, and other stakeholders; and
- Management surveillance and oversight of compliance to policies and procedures.

The depth and complexity of Anderson-Negele's incident response activity are commensurate with the potential or actual saturation risk, encompassing a structured workflow to:

- Confirm: understand details;
- Engage: trigger Incident Response Team if needed, others as necessary;
- Contain: take steps to prevent further damage or increase existing risk;
- Communicate: provide reports and communications paths to affected stakeholders;
- Remediate: rectify the issue as appropriate;
- Recover: undertake actions to revert damage or loss; and
- Rectify root cause: perform root cause analysis and lessons learned.

Backup and Disaster Recovery

Data backup and restoration process is maintained to help recover from data loss events. Data center is deployed with a replicated fail-over facility that is geographically disparate. Data is backed up on a weekly basis, with a mix of full, daily incremental as well as daily differential updates. Recovery time objective (RTO) and recovery point objective (RPO) of data restoration is twenty-four (24) hours.

If the Legendary™ software is unavailable for any reason, the PPR has redundant data backup and would continue to work independently providing all features needed for PMO compliance.

SANITARY BY DESIGN
ANDERSON-NEGELE

Anderson Instrument Co., Inc.
156 Auriesville Road
Fultonville, NY 12072
518-922-5315
518-922-8997 (fax)
www.anderson-negele.com

Privacy and Data Protection

Your data is stored and processed in the Rackspace data center in the United States. Your data will never be disclosed to any commercial or government entity, unless legally required to do so, to comply with a legally valid and binding order, such as a subpoena or a court order, or as is otherwise required by applicable law.

Human Resources Security

Newly hired personnel undergo pre-employment background checks. Processes are in place to review user IDs to verify inactive or terminated individuals are removed from Anderson-Negele systems. Security systems and supporting controls are implemented in offices to provide access control, video monitoring and auditing services.

SANITARY BY DESIGN
ANDERSON-NEGELE

Anderson Instrument Co., Inc.
156 Auriesville Road
Fultonville, NY 12072
518-922-5315
518-922-8997 (fax)
www.anderson-negele.com

Legendary™ – Information Security Controls

Best-practices are followed to ensure the confidentiality, integrity, and accuracy of data.

Data Protection

- Legendary™ data is encrypted both at rest and in transit
- Data communication between the Paperless Process Recorder (PPR) and Legendary™ data center is made via secure web service calls (HTTPS) using the Representational State Transfer (REST)
- Transport Layer Security (TLS) 1.2 encryption is used for web application and web service transmissions
- SSL certificates are issued from a reputable certificate authority (CA)
- Storage of sensitive data is limited and either encrypted or password protected at rest

Access Control

- PPR and Legendary™ implements role-based scheme to limit access and edit privilege to any system configuration
- All users must authenticate themselves in the PPR before adding or editing any system information
- Authorization in the Legendary™ is managed through role, license type, location, group, and other factors.

Authentication

- Credentials are not stored directly within application code
- Database credentials are securely stored and protected
- Generic responses are provided for authentication failures
- User accounts in the Legendary™ can be managed in following ways:
  - **Form-based authentication**: The Legendary™ account policy feature allows for the definition of password complexity requirements for a minimum number of upper-case characters, minimum number of lower case characters, minimum number of digits, minimum number of special characters, minimum length, expiry, remembering the users' previous passwords and number of invalid login attempts.