CleaverBrooks®

prométha®

Connected Boiler Solutions

Security

Frequently Asked Questions

Customer Data Protection

1. **How do you protect customer data gathered from the device?**
   Our unique design maintains absolute control over the one-way flow of data from the PLC device to the secure Cleaver-Brooks (C-B) cloud. Only Prometha devices are permitted to connect to the secure C-B cloud, and a firewall in our private cloud protects its global infrastructure.

2. **How do you ensure continued security?**
   Our cloud-provided security controls are aligned to leading standards, and we are fastidious about maintaining these standards and adhering to recommended upgrades. In addition, we actively monitor security and logging tools.

3. **Do you encrypt your data in transit?**
   Yes, all data is encrypted in transit.

4. **Do you encrypt your data at rest?**
   We do not store any data on the Prometha device.

5. **How do you verify your security?**
   We have performed penetration testing and received a letter of attestation from a third-party security firm regarding our security practices.

Cellular Network

6. **How does Cleaver-Brooks plan to maintain a secure cellular network?**
   C-B has taken several steps, including:
   - Restricting the cellular network exclusively to the Prometha device.
   - Transmitting all data over a secure encrypted tunnel between the Prometha device and our secure C-B cloud.
   - Utilizing device patching via a secure tunnel between the Prometha device and the C-B cloud.

7. **How does Cleaver-Brooks ensure a secure connection?**
   Authenticated users can only gain access to information via an encrypted, browser-based connection.

Controlled Access

8. **How does Cleaver-Brooks protect information gathered and stored on the monitoring device?**
   Each Prometha device has a unique identifier and firewall to prevent unauthorized access. The only information stored on the device is the boiler serial number and connection information to enable communication with the boiler.

(continued)

9. **How do you protect a customer's network against a cyberattack?**
   Cleaver-Brooks is using a secure cellular connection to collect customer data. Information will never travel over a Wi-Fi or Bluetooth connection, nor is there any need for Cleaver-Brooks to connect to a customer's LAN or WAN.

10. **How do you control who has access to our account?**
    Each account is set up with a unique username and password that limits access only to the account owner's boiler information. Passwords are encrypted in our database.

11. **How do you manage multiple users who may have different job functions?**
    We actively manage the security access of users based on their roles. Administrative as well as user access is granted based on the customer's desired configuration.

Ver.04