Fortress Keystone Web Portal Privacy and Data Security Policy

Last Updated: [2026-3-17]

Fortress Power LLC ("Fortress Power" or "Company") respects your privacy and is committed to protecting the personal and proprietary information you share through the Fortress Keystone Web Portal. This Privacy and Data Security Policy ("Policy") describes the information we collect, how it is used, the conditions under which it may be disclosed, and the safeguards applied to protect such information.

Fortress Power certifies that its data privacy and protection practices are designed to comply with Regulation 9246 and all applicable requirements of the Puerto Rico Energy Bureau.

---

1. Information We Collect

When you use the Fortress Keystone Web Portal, Fortress Power may collect the following categories of information:

a. Personal Information

- Name
- Email address
- Company or installer affiliation
- Phone number (if provided)

b. Account and Usage Information

- Login history and access logs
- Actions taken within the portal (e.g., viewing sites, updating settings)

c. System and Site Data

- Site names, addresses, and serial numbers
- Equipment status, alarms, and performance data
- Firmware version and device connectivity

Fortress Power does **not** collect or store sensitive personal identifiers such as Social Security numbers, payment card information, or homeownership documentation.

---

2. How We Use Your Information

Fortress Power uses customer information solely for legitimate business and operational purposes, including:

- Operating and maintaining the Fortress Keystone Web Portal
- Monitoring, diagnosing, and troubleshooting energy systems
- Providing alerts, notifications, and operational updates
- Improving system reliability, performance, and functionality
- Administering energy programs or services in which the customer has enrolled

Fortress Power processes customer information only where there is a valid legal basis, including customer consent, contractual necessity, compliance with legal obligations, or legitimate operational purposes.

Fortress Power limits the collection and use of customer information to the **minimum amount necessary** to achieve these purposes.

Fortress Power does **not** sell customer information or use personal information for advertising purposes.

---

3. Access to Information

Access to customer information is restricted to:

- Authorized Fortress Power personnel with a legitimate business need
- System administrators and technical support personnel
- Approved partners and installers, limited to assigned customer sites

All personnel with access to customer information are required to comply with Fortress Power's confidentiality and data protection requirements and are subject to access controls, monitoring, and enforcement measures.

---

4. Restrictions on Disclosure of Customer Information

Fortress Power maintains strict controls governing the disclosure of private and proprietary customer information.

4.1 Prohibition on Marketing Use of Customer Information

Fortress Power **shall not disclose** private or proprietary customer information to its affiliates, subsidiaries, or any third party **for the purpose of marketing services or product offerings to a retail electric customer who does not already subscribe to that service or product**, in accordance with Section 6.01(D)(3) of Regulation 9246.

This prohibition applies to all forms of disclosure, whether direct or indirect, and includes:

- Targeted marketing
- Customer profiling
- Lead generation
- Data analytics intended to support marketing activities

Customer information may only be used or disclosed as necessary to:

- Provide requested services
- Operate and maintain Fortress Power systems
- Administer customer-enrolled programs
- Comply with legal and regulatory obligations

4.2 Third-Party Confidentiality and Non-Disclosure Requirements

Any contract or agreement between Fortress Power and a third party involving access to customer information **shall expressly prohibit** the third party from:

- Disclosing customer information to any entity that is not Fortress Power and not a party to the contract
- Selling, renting, or otherwise monetizing customer information
- Using customer information for any purpose other than the services authorized by Fortress Power

These requirements are implemented in accordance with Section 6.01(D)(4) of Regulation 9246.

All third parties must:

- Maintain strict confidentiality of customer information
- Implement administrative, technical, and physical safeguards no less protective than those used by Fortress Power
- Use customer information solely for authorized and limited purposes

Fortress Power reserves the right to **audit, monitor, or require documentation** demonstrating third-party compliance with these obligations.

---

5. Customer Contractual Consent for Demand Response Programs

Fortress Power's data practices comply with all data-related provisions contained in Demand Response program agreements.

By enrolling in a Demand Response program, customers authorize Fortress Power to collect, use, and disclose information as explicitly described in the applicable agreement.

Any disclosure of customer information in connection with Demand Response programs shall:

- Be strictly limited to what is necessary for administration, operation, measurement, verification, or compliance
- Remain subject to all confidentiality and data protection requirements
- Comply fully with the restrictions set forth in this Policy

---

6. Your Privacy Rights

Customers may request:

- Access to personal data maintained by Fortress Power
- Correction of inaccurate or incomplete information
- Deletion of personal data where applicable under law

Fortress Power will:

- Acknowledge requests within **10 business days**
- Respond within **30 calendar days**, unless additional time is permitted by law

Requests may be submitted to:
software_admin@fortresspower.com

Fortress Power may take reasonable steps to verify the identity of the requestor prior to fulfilling any request.

If a customer believes their information has been used or disclosed in violation of this Policy, they may submit a complaint. Fortress Power will investigate and respond in accordance with its Customer Complaint Procedure.

Residents of certain jurisdictions, including Puerto Rico and California, may have additional rights under applicable law.

---

7. Data Security

Fortress Power implements comprehensive safeguards to protect customer information, including:

- Encryption of data in transit and at rest
- Access controls and authentication mechanisms
- Role-based access controls (RBAC)
- System monitoring, logging, and security auditing
- Incident detection and response systems
- Regular security updates and vulnerability management

---

8. Changes to This Policy

Fortress Power may update this Policy periodically to reflect operational, legal, or regulatory changes.

Material updates will be posted on the applicable platform, and the “Last Updated” date will be revised accordingly.

---

9. Data Retention

Fortress Power retains customer information only for as long as necessary to:

- Fulfill the purposes described in this Policy
- Comply with legal and regulatory obligations
- Resolve disputes and enforce agreements

When no longer required, information will be securely deleted, anonymized, or de-identified in accordance with applicable law and industry standards.

---

10. Data Security Incident Response

In the event of unauthorized access to customer information, Fortress Power will:

- Promptly investigate and contain the incident
- Take appropriate corrective actions
- Notify affected individuals and regulatory authorities as required by law

---

11. Children's Privacy

The Fortress Keystone Web Portal is not intended for individuals under the age of 18. Fortress Power does not knowingly collect personal information from children. Any such information identified will be promptly deleted.

---

12. Governance and Accountability

Fortress Power maintains internal governance structures to ensure compliance with this Policy.

- Designated personnel oversee data privacy and security compliance
- Employees and contractors receive periodic training on data protection obligations
- Access to customer information is monitored and enforced

Violations of this Policy may result in disciplinary action, including termination of access or contractual relationships.

---

13. Data Storage and Transfers

Customer information may be stored and processed within the United States or other jurisdictions where Fortress Power or its service providers operate.

Fortress Power ensures that any transfer of customer information is subject to appropriate safeguards, contractual protections, and security controls consistent with this Policy and applicable law.