Business Continuity Policy

Ensuring Resilience and Recovery

This policy sets out how SMART ENERGY PROVIDER LLC keeps the Smart Energy Pays platform running in the United States during a disruption, and how we recover critical services when something goes wrong.

Table of Contents

- 1. Introduction
- 2. Scope and Objectives
- 3. Business Impact Analysis and Recovery Objectives
- 4. Recovery Strategies and Procedures
- 5. Roles and Responsibilities
- 6. Disaster Scenarios and Response Procedures
- 7. Training, Testing and Maintenance
- 8. Appendices
- 9. Next Review

1. Version Control

Document Title	Business Continuity Policy
Company	SMART ENERGY PROVIDER LLC, a Florida limited liability company (Florida document number L25000037694)
Platform	Smart Energy Pays (www.smartenergypays.us and the Smart Energy Pays mobile app)
Principal Office	101 NE 43 St, Miami, FL 33137, United States of America
Version	2.0
Effective Date	October 6, 2026
Policy Owner	Chief Technology Officer
Approved By	Chief Executive Officer
Review Cycle	At least annually, and after any major incident or significant change to the business

SMART ENERGY PROVIDER LLC ("Smart Energy Pay", "we", "us" or "our") operates the Smart Energy Pays platform in the United States. Through the platform, customers can hold and convert supported digital assets, receive and send U.S. dollar payments, and use the Smart Energy Pays Visa® Card, which is issued by a licensed bank partner.

Our customers rely on these services every day. This policy makes sure that, if a disruption happens, we can:

- protect the safety of our people;
- protect customer funds, digital assets and data;
- keep critical services available, or restore them quickly; and
- keep customers, bank partners, service providers and regulators properly informed.

This policy supports our Information Security Policy and Incident Response Plan, and is aligned with ISO/IEC 27001:2022 controls 5.29 (Information security during disruption) and 5.30 (ICT readiness for business continuity).

2. Scope and Objectives

2.1 Scope

This policy applies to all employees, contractors and critical third-party providers that support the Smart Energy Pays platform in the United States. It covers the following areas:

- the Smart Energy Pays app, website and APIs, and the cloud infrastructure behind them;
- customer onboarding, identity verification (KYC) and account management;
- custodial digital asset wallets and blockchain infrastructure;
- the Smart Energy Pays Card program, including card management and card controls;
- U.S. dollar virtual accounts, ACH and wire payments, and digital asset conversions;
- fraud monitoring, anti-money laundering (AML) and sanctions screening;
- customer support; and
- finance, reconciliation and regulatory and partner reporting.

2.2 Objectives

- Keep critical business functions running during a disruption.
- Restore services within the recovery time objectives (RTO) and recovery point objectives (RPO) in Section 3.
- Protect the confidentiality, integrity and availability of customer data and funds at all times, including during recovery.
- Keep communication channels open with staff, customers, bank partners, service providers and regulators.
- Meet our legal, regulatory and contractual obligations, including obligations to our card issuing bank and program partners.
- Learn from every incident and test, and continuously improve this policy.

2.3 Critical Functions

Each critical function has a designated owner who is responsible for its recovery procedures.

Function	What it covers	Owner	Tier
Platform availability	App, website, APIs, authentication and core ledger	Chief Technology Officer	Tier 1
Card services	Card management, card controls (freeze/unfreeze), card funding and authorization connectivity with our card program partner	Chief Technology Officer	Tier 1
Wallet and blockchain infrastructure	Custodial wallets, signing services, blockchain nodes and transaction monitoring	Chief Technology Officer	Tier 1
Fraud, AML and sanctions screening	Transaction monitoring, sanctions screening, suspicious activity escalation	Compliance Officer	Tier 1
Customer support	Support for account access, lost or stolen cards, fraud reports and payment issues	Head of Customer Support	Tier 1
Payments and virtual accounts	ACH and wire transfers, digital asset conversions, payment operations	Head of Operations	Tier 2
Customer onboarding	Account opening and identity verification	Compliance Officer	Tier 2
Finance and reconciliation	Daily reconciliation, settlement with partners, fee collection	Head of Finance	Tier 2
Regulatory and partner reporting	Reporting to bank partners, program partners and authorities	Compliance Officer	Tier 2
Non-critical functions	Marketing, analytics, internal tools and non-customer-facing development	Function lead	Tier 3

2.4 Risk Assessment

We assess business continuity risks at least once a year, and whenever there is a significant change to our business, systems or providers. In each assessment we:

- identify threats, including natural and environmental threats, man-made threats and technical threats;
- evaluate each risk based on its likelihood and impact, using the risk matrix below;
- agree mitigation measures for every medium and high risk, and assign an owner; and
- record the results in our risk register and review them with management.

Risk Matrix

Likelihood	Insignificant	Minor	Moderate	Major	Significant
Almost Certain	Low	Medium	High	High	High
Highly Likely	Low	Low	Medium	High	High
Likely	Low	Low	Medium	High	High
Unlikely	Low	Low	Medium	Medium	High
Highly Unlikely	Low	Low	Low	Low	Medium

Risk Level	Required action
High	Treat immediately. Mitigation plan approved by management and tracked to completion.
Medium	Mitigate within an agreed timeframe and monitor.
Low	Accept and monitor through the regular risk review.

3. Business Impact Analysis and Recovery Objectives

3.1 Business Impact Analysis

The business impact analysis (BIA) identifies which processes matter most, what they depend on, and how quickly they must be restored. It also highlights gaps and single points of failure, and gives management the information needed to set recovery priorities and the business continuity budget. The BIA:

- identifies critical processes and their dependencies, both internal (people, systems, data) and external (bank partners, card program partners, payment networks, cloud and technology providers, regulators);
- assesses the impact of a disruption on customers, finances, regulatory compliance and reputation;
- determines how critical each function is and sets its recovery tier;
- identifies high-risk areas and single points of failure in our infrastructure; and
- sets recovery time and recovery point objectives, in particular for IT systems.

The BIA is reviewed at least annually, together with this policy.

3.2 Recovery Objectives

Recovery Time Objective (RTO) is the maximum acceptable time a function can be unavailable before it must be restored. Recovery Point Objective (RPO) is the maximum acceptable amount of data loss, measured in **time.**

Tier	Functions	Business Impact	RTO	RPO
Tier 1	Critical functions	Severe or major	Within 1 to 3 hours	No more than 1 hour of data loss
Tier 2	Essential functions	Moderate	Within 24 to 72 hours	No more than 24 hours of data loss
Tier 3	Desirable functions	Minor	Within 120 hours	No more than 72 hours of data loss

Where a recovery depends on a bank partner, card program partner or other third party, our recovery time may also depend on that provider's own recovery. We monitor these providers closely and escalate under our agreements with them.

3.3 Disruption Scenarios Considered

Category	Examples
Staffing	Loss of key staff through illness, accident or resignation; pandemic; key person unavailable without a trained backup
Infrastructure	Loss of access to the Miami office; power or internet outage; theft or damage of company equipment
Cyber and data	Data breach; ransomware or system intrusion; compromise of credentials or signing keys; denial-of-service attack
Third-party	Outage at our card program partner, issuing bank, banking or payment partners, identity verification provider, cloud provider, or blockchain networks
Environmental	Hurricanes and tropical storms (particularly during the Atlantic hurricane season, June to November), flooding, extreme weather and other natural disasters
Civil and other	Civil unrest, terrorism, or a government action that prevents access to facilities or services

4. Recovery Strategies and Procedures

4.1 Recovery Strategies

Area	Strategy
Cloud infrastructure	Production systems run on enterprise cloud infrastructure across multiple availability zones. Infrastructure is defined as code so it can be rebuilt quickly. Encrypted backups are kept in a separate region.
Secrets and keys	Secrets are held in a dedicated secrets management system with restricted access. Signing keys for custodial wallets are protected with strict access controls and documented, tested recovery procedures.
Wallet and blockchain	Wallet services run on persistent, monitored compute with redundant blockchain nodes. Outgoing transactions can be paused safely while an incident is investigated.
Card services	Customers can freeze and unfreeze their cards in the app at any time. If the app is unavailable, customers can freeze their card by calling the number on the back of their card.
Workforce	We are a remote-first company. Staff can work securely from any location using company-managed devices, Google Workspace and Slack, so we do not depend on a single office.
Third-party providers	Critical providers are assessed before onboarding and reviewed annually, with service levels and incident notification duties set in our agreements. Where feasible, we identify alternative providers in advance.
Customer communication	We tell customers about service disruptions through in-app notices, email and our website.

4.2 Emergency Response

Emergency response procedures start as soon as a disruption is detected:

- Make sure people are safe, and contact emergency services if needed.
- Assess the situation and its impact on customers, funds and data.
- Notify the Business Continuity Coordinator and key personnel using the contact register.
- Decide whether to declare a disaster and activate this policy.
- Start the relevant scenario procedure in Section 6 and the Incident Response Plan where security is affected.

4.3 Recovery Priorities

Once a disaster has been declared, we work through the following priorities in order:

Priority	Action
1. People	Make sure all staff are accounted for and, where possible, safe.
2. Notify	Notify management, staff, affected service providers and, where needed, emergency services.
3. Assess	Assess the impact on customers, funds, data, systems and third-party providers, including whether any customer or staff data has been compromised.
4. Protect	Take immediate steps to protect customer funds and data, for example by pausing affected services, revoking access or rotating credentials.
5. Mobilize	Confirm the Emergency Response Team is available, and activate backup personnel for anyone who is unavailable.
6. Restore critical	Restore Tier 1 functions within their RTO.
7. Communicate	Keep customers, partners and, where required, regulators informed.
8. Restore remaining	Restore Tier 2 and Tier 3 functions and confirm full service.

4.4 Recovery Plan Phases

Phase	What happens	Key activities
1. Disaster occurrence	From the moment of the event until management activates the plan	Emergency response; notification of relevant parties; damage and impact assessment; declaration of disaster
2. Plan activation	Recovery teams put their procedures into action	Assemble recovery team; implement interim procedures; move to remote or alternate working; re-establish communications
3. Alternate operations	Business runs from alternate locations or systems	Run critical functions; monitor service levels; daily status reporting; track costs
4. Return to normal	Business returns to normal operations	Move back to primary systems or location; verify data integrity; declare disaster over; post-incident review

4.5 Relocation and Alternate Work Locations

Primary Location	Alternate Arrangement
101 NE 43 St, Miami, FL 33137 (principal office)	All staff work remotely using company-managed devices
Remote staff home locations	Another safe location with secure internet access, or temporary coverage by a backup team member

For long-term disruptions, staff will continue working remotely until the primary office, or a suitable replacement, is available.

4.6 Vital Records and Backup

- Business records, email and documents are stored in Google Workspace, which keeps data in multiple data centers to limit the impact of any local disaster.
- Production databases and systems are backed up automatically. Backups are encrypted, kept in a separate region, and restored in regular tests.
- Customer, transaction and compliance records are kept for at least five years, or longer where required by law or by our partners.
- Staff must save work documents in approved cloud storage, not only on local devices, so that the loss of a device does not mean the loss of records.
- Any paper records created during a disruption must be digitized or securely stored once the disruption is over, in line with our confidentiality and record retention policies.

4.7 Access to Systems During a Disruption

- Systems are cloud-hosted, so authorized staff can access them securely from company-managed devices wherever they are, using multi-factor authentication.
- If a key staff member cannot perform their duties, their designated backup takes over remotely.
- During a cyber incident, staff must not access or change affected systems until the Chief Technology Officer confirms it is safe.

4.8 Customer Support Continuity

- Customers can contact us through in-app support and by email at support@smartenergypays.us.
- Customers can freeze their card in the app, or by calling the number on the back of the card if the app is unavailable.
- Reports of lost or stolen cards, unauthorized transactions and fraud are prioritized over all other requests.
- During a disruption, we publish status updates in the app and on our website, and we tell customers when service has been restored.

4.9 Communication Plan

Audience	When	How	Owner
Staff	As soon as a disaster is declared, then at least daily	Phone, Slack, email, WhatsApp	Business Continuity Coordinator
Customers	When a disruption affects them, with regular updates until it is resolved	In-app notice, email, website	Communications Lead
Card issuing bank and card program partner	Promptly, and within the timeframes required by our agreements	Agreed incident channels	Chief Technology Officer
Banking, payment and other critical providers	Promptly, where they are affected or needed for recovery	Agreed incident channels	Chief Technology Officer / Head of Operations
Regulators and law enforcement	As required by applicable law	As required	Compliance Officer
Media and public	Only when approved by the CEO	Approved statements	Chief Executive Officer

Only the Chief Executive Officer, or staff the CEO authorizes, may make statements to the media or the public.

5. Roles and Responsibilities

5.1 Purpose

This section describes who takes part in recovery. The Business Continuity Coordinator leads the recovery effort, delegates tasks, supports team members and reports to the executive team on progress and expected recovery times. Every key role has a designated backup.

5.2 Roles and Responsibilities

Role	Responsibilities
Chief Executive Officer	Approves this policy; declares a disaster together with the Business Continuity Coordinator; approves all external statements; keeps the board and owners informed.
Chief Technology Officer (Policy Owner)	Owns this policy; leads IT and security recovery; activates the Incident Response Plan; coordinates with cloud, technology and card program partners; reports recovery status to the executive team.
Business Continuity Coordinator (Team Leader)	Coordinates the overall recovery effort; is the main point of contact until the disaster is declared over; monitors progress and reports to staff and executives daily; keeps a record of all disaster-related costs.

Backup Team Leader	Knows this policy well and takes over from the Business Continuity Coordinator if needed; helps prepare reports and coordinate teams.
IT and Engineering Recovery Team	Restores systems from backups; mobilizes IT resources; coordinates with technology providers; tests restored systems; keeps the CTO informed.
Compliance Officer	Makes sure AML, sanctions and fraud controls continue during the disruption; handles any required notices to regulators and partners; documents compliance-related decisions.
Communications Lead	Prepares customer and partner communications with the CEO's approval; coordinates updates to customers, providers, regulators, insurers and other stakeholders.
Head of Customer Support	Keeps customer support running; prioritizes urgent cases such as lost cards and fraud; makes sure support staff have up-to-date information.
Human Resources	Informs staff and, where needed, their families; notifies emergency contacts of injury; arranges travel and expense support; handles insurance claims.
Administration and Finance	Tracks recovery costs; arranges supplies, equipment and travel; coordinates with facilities and vendors on repairs.
Emergency Response Team	Focuses on staff safety; assesses damage where it is safe to do so; prepares impact assessments for the executive team.
Team Members	Follow instructions from team leaders; carry out their normal duties where possible; report on completed work.

5.3 Staff Notification

When a disaster is declared, the Business Continuity Coordinator notifies department heads and team leaders, who then notify their own teams (the phone tree). Contact details are kept in the internal emergency contact register (Appendix A). If phone lines are unavailable, we use the backup channels in Appendix B. The phone tree is tested every quarter.

5.4 External Contacts

The Business Continuity Coordinator keeps an up-to-date list of key external contacts, including our card issuing bank, card program partner, banking and payment providers, identity verification provider, cloud and technology providers, insurers and legal counsel. The list includes both business-hours and emergency contact details and is available to the Emergency Response Team in our secure shared drive.

6. Disaster Scenarios and Response Procedures

Staff safety always comes first. Disasters are rarely the same twice, so some deviation from these procedures is expected, but staff should be familiar with them and follow them as closely as possible.

Scenario	Example events	Target RTO	Lead
A. Loss of office or work location	Fire, power outage, theft, civil unrest or transit disruption preventing access	1 to 2 business days	Business Continuity Coordinator
B. Cyber or data incident	Data breach, ransomware, system intrusion, credential or key compromise	Tier 1 functions within 1 to 3 hours	Chief Technology Officer
C. Critical third-party outage	Outage at card program partner, issuing bank, payment provider, KYC provider, cloud provider or blockchain network	In line with provider recovery and Section 3	Chief Technology Officer
D. Environmental event	Hurricane, flooding or other natural disaster	1 to 2 business days	Business Continuity Coordinator
E. Loss of key staff	Illness, accident, death or departure of key staff	1 to 2 business days	Business Continuity Coordinator / HR

6.1 Scenario A: Loss of Office or Work Location

Step	Activity	Performed by
1. Confirm location is unavailable	Evacuate safely if on site; inform emergency services where needed; confirm all staff are safe; contact building management	Business Continuity Coordinator
2. Declare disaster	Inform executives and staff by phone or email; notify HR of any injury so emergency contacts can be informed	Business Continuity Coordinator
3. Move to remote working	Confirm staff can work remotely and have the equipment they need; provide replacement devices; arrange cover for anyone who cannot work	Business Continuity Coordinator / IT
4. Check third parties	Confirm partners and providers are not affected; get system status from IT; note impacts in daily status reports	Business Continuity Coordinator
5. Keep critical functions running	Follow up with internal and external stakeholders; report progress to executives daily; track costs	Business Continuity Coordinator and Emergency Response Team
6. Return to normal	Return to the primary or a replacement location; secure any paper records; monitor performance and escalate issues	Business Continuity Coordinator and all staff
7. Declare disaster over	Notify executives and staff that the disaster is over and start the post-incident review	Business Continuity Coordinator

6.2 Scenario B: Cyber or Data Incident

Step	Activity	Performed by
1. Confirm the incident	Confirm with the CTO or the on-call engineer that an incident has happened. Use phone where other systems may be compromised.	Business Continuity Coordinator
2. Contain	Activate the Incident Response Plan; isolate affected systems; pause affected services such as outgoing wallet transactions where needed; revoke compromised access and rotate credentials and keys	Chief Technology Officer and IT Recovery Team
3. Declare disaster	Inform executives and staff; tell staff not to use or change affected systems until IT confirms it is safe	Chief Technology Officer
4. Notify partners and authorities	Notify our card program partner, issuing bank and other affected providers within the timeframes in our agreements; assess legal notification duties, including data breach notices to customers and state authorities	Chief Technology Officer and Compliance Officer
5. Recover	Restore systems from clean backups; verify data integrity and reconcile balances and transactions before restarting services	IT Recovery Team and Head of Finance
6. Resume service	Restart services once secure; inform customers; monitor closely for further suspicious activity	Chief Technology Officer
7. Declare disaster over	Notify executives that the incident is closed; complete a post-incident report and corrective actions	Chief Technology Officer

6.3 Scenario C: Critical Third-Party Outage

Step	Activity	Performed by
1. Confirm the outage	Confirm the outage with the provider through agreed incident channels and check its status page	Chief Technology Officer
2. Assess impact	Identify which customer services are affected, for example card transactions, payments or onboarding	Chief Technology Officer and Head of Operations
3. Protect customers	Show in-app notices; switch to an alternative provider where one is available; pause affected features where needed to protect customer funds	Chief Technology Officer
4. Communicate	Keep customers informed; escalate with the provider under our agreement; keep the executive team updated	Communications Lead
5. Recover and reconcile	Once the provider recovers, process queued items and reconcile all transactions and balances	Head of Operations and Head of Finance
6. Review	Review the provider's incident report and decide whether further action is needed	Chief Technology Officer and Compliance Officer

6.4 Scenario D: Environmental Event

Step	Activity	Performed by
1. Prepare	When a hurricane or severe weather warning is issued for Miami or another staff location, confirm remote working readiness, charge devices and check backup communication channels	Business Continuity Coordinator
2. Confirm location is unavailable	Evacuate safely; follow official emergency instructions; confirm staff are safe and can reach a safe place	Business Continuity Coordinator
3. Declare disaster	Inform executives and staff; notify HR of any injury	Business Continuity Coordinator
4. Continue operations	Move affected staff's duties to team members in unaffected locations; provide replacement equipment; track costs	Business Continuity Coordinator and team leaders
5. Check third parties	Contact partners and providers to assess impact; get system status from IT	Business Continuity Coordinator
6. Return to normal and declare disaster over	Return to normal working; secure any records; notify executives and staff that the disaster is over	Business Continuity Coordinator

6.5 Scenario E: Loss of Key Staff

Step	Activity	Performed by
1. Confirm the situation	Confirm that the employee is unable to work and, where possible, for how long; if the employee has left, disable all system access immediately	Business Continuity Coordinator / HR
2. Declare disaster	Inform the executive team	Business Continuity Coordinator
3. Activate backup	Contact the employee's manager or designated backup and hand over their duties	Business Continuity Coordinator
4. Use documentation	Use documented processes and procedures in the shared drive; introduce the backup to external contacts	Employee's manager
5. Keep work moving	Check that the backup's workload is manageable; reassign or pause non-critical tasks	Employee's manager
6. Succession or recruitment	Promote internally or recruit; train the new person	HR
7. Declare disaster over	Inform the executive team	Business Continuity Coordinator

7. Training, Testing and Maintenance

7.1 Training and Awareness

Training	Frequency	Participants
Business continuity awareness	Annually and at onboarding	All staff
Role-specific recovery training	Annually, and when roles change	Emergency Response Team and key personnel
Incident response and emergency procedures	Annually	All staff

7.2 Testing

Test	Frequency	Responsible
Tabletop exercise of one or more scenarios in Section 6	Annually	Business Continuity Coordinator
Infrastructure recovery and failover test	Annually	Chief Technology Officer
Backup restore test	Monthly	IT and Engineering
Phone tree and contact register check	Quarterly	Human Resources
Key staff backup test (backup performs the role for a set period)	Annually	Business Continuity Coordinator

Test results are recorded, compared against the RTO and RPO in Section 3, and any gaps are logged as corrective actions with an owner and a due date.

7.3 Plan Maintenance and Distribution

The Chief Technology Officer is responsible for maintaining this policy. It is reviewed at least once a year, and also after any major incident, test finding, or significant change to our business, systems or providers. The current version is available to all staff in our secure shared drive and is distributed to:

Team	Title	Location
Executive	Chief Executive Officer	Miami, FL
Technology	Chief Technology Officer	Remote
Compliance	Compliance Officer	Remote
Operations and Finance	Head of Operations / Head of Finance	Remote
Customer Support	Head of Customer Support	Remote

8. Appendices

Appendix A: Emergency Contacts

Names, personal phone numbers and emergency contact details of staff are kept in the internal emergency contact register, which is stored securely and reviewed every quarter. They are not published in this policy.

Role	Contact
Chief Executive Officer	dd@smartenergypay.com
Chief Technology Officer	development@smartenergypay.com
Legal and Compliance	legal@smartenergypay.com
Customer Support	support@smartenergypays.us
Mail	SMART ENERGY PROVIDER LLC, 101 NE 43 St, Miami, FL 33137, United States of America

Appendix B: Backup Communication Channels

- Phone and SMS
- Email (Google Workspace)
- Slack
- WhatsApp
- Customer support platform, for customer communications

Appendix C: Function Recovery Summary

Function	Recovery procedure	Responsible
IT systems and platform	Restore from backups or fail over to alternate infrastructure	Chief Technology Officer
Wallet and blockchain	Pause outgoing transactions if needed; recover services and keys under documented procedures; reconcile balances	Chief Technology Officer
Card services	Coordinate with the card program partner; keep in-app and phone card freeze available	Chief Technology Officer
Fraud, AML and sanctions	Continue monitoring; switch to manual review if automated tools are down	Compliance Officer
Customer support	Activate backup support team; publish status updates	Head of Customer Support
Payments and finance	Switch to backup procedures; reconcile all transactions after recovery	Head of Operations / Head of Finance

9. Next Review

- October 2027, or earlier if required by a major incident or significant change.