CONVENIENCE PAY TECHNOLOGIES LTD.

Convenience Pay Technologies Ltd.

Automated Vehicle Fueling Policy

CPTL-AVF-POL-0001

Table of Contents

1.0 TITLE: CONVENIENCE PAY AUTOMATED VEHICLE FUELING POLICY

2.0 PURPOSE

The purpose of this policy is to establish a comprehensive framework for the efficient and secure provision of fuel services to vehicle owners through an automated and mobile phone-based platform. This policy aims to streamline the fueling process, enhance user experience, ensure safety and environmental compliance, and promote the responsible use of automated fueling technology.

By defining clear guidelines, procedures, and standards, this policy seeks to create a reliable and convenient fueling solution that aligns with emerging technological advancements while prioritizing safety, sustainability, and customer satisfaction.

3.0 SCOPE

This Policy applies to all stakeholders of the Automated Vehicle Fuelling Solution, including the following:

- Technical Support Staff
- Compliance Officers
- Sales and Marketing
- Cybersecurity Team
- Customer Support Representatives
- Management and Decision-makers
- Software Developers
- Merchants
- Customers

4.0 TERMS AND DEFINITIONS

Term	Definition
Automated Vehicle Fueling	A convenient and technology-driven service, offered by Convenience Pay Technologies Ltd. that allows users to request and receive fuel directly to their vehicles at an onboarded gas station of their choosing
Customers	Individuals or entities who are onboarded and utilize the Automated Vehicle Fuelling application

Term	Definition
E-Money	A digital alternative to cash, allowing users to make cashless payments with money stored electronically, which can be accessed via a mobile device
Merchants	Businesses or individuals who own or operate gas stations and who are onboarded with the Automated Vehicle Fuelling application.
Payment Processor	The service provider responsible for connecting the necessary payment networks and financial institutions involved in the transaction to ensure the smooth and secure processing of payments in online and offline transactions.

5.0 RESPONSIBILITIES

Owner	Responsibility
Compliance Department	• Ensure compliance with all relevant laws and regulations. Review and update the policy as needed to reflect changes in the legal and regulatory environment.
Customer	• Use the Automated Vehicle Fueling app in accordance with the policies and guidelines set forth by Convenience Pay Technologies Ltd. • Provide feedback on the service and report any issues or concerns to Customer service.
Customer Service	• Ensure that Customer inquiries and complaints are handled promptly and professionally. Monitor Customer feedback and use it to improve the service.
Finance	• Ensure that the fee structure is fair and competitive. Monitor the financial performance of the application and take corrective action if needed.
Information Security/ Cyber Security	• Ensure that the payment system is secure and that user data is protected. Monitor the system for potential security breaches and take corrective action if needed.
International Business Growth, Digital and Brand Experience (IBGDBE)	• Develop and implement marketing strategies to promote the Automated Vehicle Fueling app. Ensure that all marketing materials are ethical and truthful.
Product Development	• To continuously improve the service. Seek feedback from Customers to identify areas for improvement.

6.0 POLICY

The Automated Vehicle Fueling application is an application offered by Convenience Pay Technologies Ltd. (hereby known as Convenience Pay), which allows consumers to pay for fuel by activating the dispenser from their mobile device. From the app, Customers have the ability to select their preferred location, pump number, type of fuel and quantity/price requested. Upon confirmation of these variables, they then enter a unique code at the pump to start fueling.

The Automated Vehicle Fueling app shall support multiple convenient payment methods for Customers, including, but not limited to, credit cards, debit cards and the Convenience Pay Digital Wallet. The app shall be used for the purchase of Diesel, Super and Premium Unleaded fuel only, and not for the purchase of CNG.

6.1 Enrollment

6.1.1 Merchant Enrollment

Merchants shall be required to undergo a registration process in which the following is confirmed:

- the legitimacy of their business/ company, supported by the submission of documentation, for example registration certificate, licenses, permits, and any other legal documentation specific to their industry or region, for evaluation by Convenience Pay.
- The authorization of their company to distribute fuel

Merchants satisfying the criteria shall be required to enter into an agreement with Convenience Pay, for the use of the Automated Vehicle Fueling app at their service station locations, and ensure compliance with usage guidelines, service fees, and any other provisions specified in the agreement between the Merchant and Convenience Pay.

6.1.2 Customer Enrollment

Customers shall be required to enroll in this app, through a quick and easy registration process. They shall be required to fill out the in-app registration form and accept the terms of use in order to be onboarded.

6.2 Technical Design Elements

6.2.1 Alerts and Notifications

Clear visual and audible alerts shall be implemented that are easily distinguishable and intuitive to understand, as follows:

i. **Transaction Timer:** Upon receipt of the four-digit code, a timer is initiated and counts down the allotted time to activate the dispenser. Users will receive alerts on their mobile device, as the timer approaches expiration. Notifications will be designed to provide sufficient time for users to start the fueling transaction.

ii. **Service Interruptions:** These alerts should promptly capture the attention of users and convey the occurrence of a service interruption during a transaction. The visual elements, such as colors, icons, and messages, shall be carefully chosen to provide maximum clarity and minimize confusion.

   Visual alerts shall clearly differentiate between different types of service interruptions. For example, if a service interruption occurs during a transaction, the visual alert should provide specific clarification on whether the transaction failed or is pending completion. This differentiation helps users understand the status of their transaction accurately and guides them on the appropriate next steps.

iii. **Transaction Completion:** Customers shall be notified of successful or failed transactions.

6.2.2 Compatibility

The Automated Vehicle Fueling application is designed to be compatible and integrate with the fuel dispenser. Integration tests shall be conducted to ensure a robust and reliable connection between the application and the dispenser, allowing for efficient and secure transactions.

6.2.3 Testing

A dedicated test environment shall be maintained to facilitate comprehensive testing of the Automated Vehicle Fueling app across different platforms and configurations. This environment shall be equipped with the necessary hardware, software, and configurations and shall closely resemble the production environment to replicate real-world scenarios accurately. The following types of testing shall be performed:

i. Functionality testing shall be conducted to validate that the app functions as intended by verifying that all features and functionality work as specified in the requirements and design documents, meeting the needs of users, and operating according to the expected behavior.

ii. Regression testing shall be conducted to verify that any modifications or enhancements made to the app do not introduce unintended side effects or break existing functionalities, and that all previously implemented features continue to work as expected after the changes have been made.

iii. Stress testing shall be conducted to evaluate the performance and stability of the app under high-volume transaction scenarios, simulating a significant increase in transaction volume to assess how the system handles the load.

Proper change-control procedures shall ensure the promotion of only fully tested and approved changes into the production environment. This shall include regression testing and shall ensure that only specified signatures allow the change to be promoted into the production environment.

6.3 Fuel Theft Prevention

In order to minimize the risk of fuel theft and ensure the secure management of fuel resources, the organization adopts the following policy:

i. **Unique Code Generation:** Upon the successful purchase of fuel through the mobile application, a unique and time-sensitive code shall be generated and associated with the transaction, and the pump reserved, awaiting entry of the unique code.

ii. **Code Delivery:** The unique code shall be securely delivered to the Customer through the mobile application, ensuring that only the authenticated user has access to the code.

iii. **Time Sensitivity:** The generated code will be time-sensitive, with a predefined expiration period. Customers must enter the code at the pump within the specified time frame to dispense fuel, adding an extra layer of security.

iv. **Dispenser Authentication:** Fuel dispensers will be equipped with authentication systems that prompt users to enter the unique code before fuel is dispensed. Dispensers will only activate upon successful verification of the valid code.

6.4 Full Service

In order to provide a comprehensive and convenient user experience, Convenience Pay shall offer a Full-Service feature within the mobile application, available at some locations. This feature shall enable customers to order additional services along with fueling. The following policies outline the implementation and management of the Full-Service feature:

i. **Service Menu:** The mobile application will present a user-friendly service menu that lists a range of additional services including, but not limited to, car wash, tire air check, tire patching, windscreen cleaning, and oil replenishment. The service menu may be expanded or modified based on user feedback and business requirements.

ii. **Transparent Pricing:** Clear and transparent pricing for each additional service will be displayed within the mobile application. Customers will be informed of the cost associated with each selected service before confirming their order.

iii. **Service Provider Verification:** The organization will partner with reputable service providers to deliver high-quality services. Service providers will undergo verification processes to ensure their reliability, professionalism, and adherence to service standards.

iv. **Service Availability:** The Full-Service feature will be available during specified operating hours, and service providers will be dispatched promptly upon order confirmation. Users will be informed of service availability based on their location and the operating hours of partnered service providers.

v. **Safety and Compliance:** Additional services involving vehicle maintenance or handling of automotive products will adhere to safety standards and regulatory requirements. The organization will collaborate with service providers to ensure compliance with industry regulations.

6.5 Security and Compliance

Convenience Pay is committed to providing a secure and reliable payment experience for its Customers, through protecting sensitive information during transactions. Therefore, the following policy has been established to guide all parties involved in the transaction flow, including Convenience Pay and the Payment Processor, in the implementation of strong data security measures.

6.5.1 Data Protection

Convenience Pay shall ensure that itself and the Payment Processor adhere to industry-standard encryption protocols to safeguard Customer data from unauthorized access, fraud, and data breaches. This includes utilizing robust encryption algorithms, such as Secure Sockets Layer (SSL), to encrypt data transmitted along the transaction flow.

All communication channels involved in the transaction flow shall use secure transmission methods to protect data in transit. This includes using encrypted connections (HTTPS) for data exchange between the app and the Payment Processor.

Convenience Pay shall ensure that itself and the Payment Processor shall only collect and retain Customer data that is essential for completing the transaction. Unnecessary or sensitive information shall not be stored unless explicitly required by applicable laws or regulations. Any stored data shall be properly secured and protected from unauthorized access.

6.5.2 Compliance

Convenience Pay shall ensure that the Payment Processor complies with the Payment Card Industry Data Security Standard (PCI DSS). This comprehensive security standard ensures the protection of cardholder data during payment transactions. Compliance with PCI DSS includes maintaining a secure network, implementing robust access controls, regularly monitoring and testing systems, and maintaining an information security policy.

Convenience Pay shall also ensure compliance with the rules and regulations of the Ministry of Energy and Energy Industries (MEEI) and any other regulatory requirements.

6.5.3 Authentication and Verification Protocols

Measures shall be implemented for the various interfaces, to ensure that users create strong and unique passwords that meet specific complexity criteria. Industry-standard best practices shall be employed for securely storing user passwords.

Users shall be prompted to periodically change their passwords to minimize the risk of unauthorized access. Password expiration policies shall be enforced, in alignment with the company's Cybersecurity policy.

6.5.4 Cybersecurity

Vulnerability assessments and penetration testing shall be conducted prior to implementation, before any major updates, and periodically, to identify and address any security weaknesses in the app. Convenience Pay shall ensure that itself and the Payment Processor promptly apply security patches and updates to mitigate vulnerabilities and ensure the overall security of the system.

Convenience Pay shall select a third party to perform the Vulnerability Assessment and shall ensure that said party has demonstrated success in ethical hacking practices, including having a track record of identifying vulnerabilities, conducting penetration testing, and providing actionable recommendations for remediation. The selection shall involve:

i. The employment of robust selection criteria which includes the reputation and trustworthiness of the potential assessment provider, their professional integrity, adherence to ethical standards, and compliance with relevant regulations. Only parties with a proven track record of maintaining confidentiality and upholding ethical standards shall be eligible for consideration.
ii. Comprehensive background and reference checks, involving the verification of the credentials and reputation of the potential assessment provider, and confirming with past clients any successful cyber-attacks they may have experienced since working with the provider.
iii. Evaluation of the cybersecurity expertise of the potential assessment provider, including their knowledge of industry best practices, emerging threats, and regulatory requirements.
iv. Confirmation of demonstrated commitment to following recognized methodologies, industry standards and best practices in conducting vulnerability assessments.

The selected party shall be required to sign a confidentiality and non-disclosure agreement to protect the confidentiality of the Company's sensitive information throughout the assessment process. This ensures that all findings and vulnerabilities identified during the assessment are treated with the utmost discretion and are not disclosed to any unauthorized parties.

6.6 Back-up/Recovery Plan

A comprehensive and robust Business Continuity Plan shall be maintained that outlines the steps and procedures to recover and restore services in the event of a disruption. The plan shall include the defined roles and responsibilities, procedures and actions required to recover critical systems, data, and operations in a timely manner. The plan shall be periodically reviewed, updated, and tested where possible to ensure its effectiveness.

6.7 Safety

6.7.1 In-App Safety Guidelines

All users of the Automated Vehicle Fueling app are required to adhere to the in-app safety guidelines, which emphasizes the importance of focusing on the refueling task, by selecting a checkbox after reading the guidelines. Effective communication strategies shall be used to educate Customers on best safety practices, as follows:

i. **Prioritize Refueling Tasks:** When engaged in the refueling process, users shall prioritize and concentrate solely on the task at hand. Distractions, such as using other app features or devices, shall be avoided during refueling.

ii. **Minimize Multitasking:** Users shall avoid multitasking while refueling. The app interface shall be used exclusively for monitoring and managing the refueling process, with full attention dedicated to completing it safely and efficiently.

iii. **Stay Alert to Surroundings:** App usage should not distract users from awareness of their surroundings and any potential hazards. Any unusual circumstances must be reported immediately.

iv. **Follow App-Provided Instructions:** Users shall follow the in-app instructions related to the refueling process. Any deviation from these guidelines may compromise safety and should be avoided.

v. **Report Issues Promptly:** If users encounter any issues or uncertainties during the refueling process, they are encouraged to report them promptly. This includes technical glitches, safety concerns, equipment malfunction, or any other anomalies that may compromise the safe and accurate completion of the task.

vi. **Designated Areas for App-Usage:** The Automated Vehicle Fueling app shall not be used at CNG dispensers or in any designated hazardous areas (as identified in section 6.7.3).

In addition to these safety guidelines, Customers shall adhere to the normal safety guidelines for vehicle refueling and service station protocol.

6.7.2 Forecourt Signage and Mobile Phone Usage

To enhance safety and streamline the refueling experience, users shall be required to adhere to the forecourt signage guidelines, which illustrate the use of mobile phones for payment and restricts their other usage while fueling at the dispenser. The following policies shall be in effect:

i. **Clear Forecourt Signage:** Clear and prominently placed forecourt signage shall be provided at each dispenser, illustrating the approved use of mobile phones for payment purposes only in the Automated Vehicle Fueling app. Users are required to review and comply with these guidelines before initiating any transaction in the app.

ii. **Mobile Phones Usage:** The use of mobile phones while at the dispenser is limited to payment transactions only and must be done while inside the parked vehicle.

iii. **Prohibition of Usage While Fueling:** It is strictly prohibited to use mobile phones for any purpose, including calls, messaging, or app usage, while actively fueling at the dispenser. All mobile devices must be stowed or set aside to minimize distractions and potential safety hazards.

iv. **Enforcement of Policy:** Forecourt attendants shall monitor customers to ensure compliance with this policy. Users found in violation of the mobile phone usage prohibition may be subject to warnings, account suspensions, or other appropriate disciplinary actions.

v. **Education and Awareness:** Regular awareness campaigns and educational materials shall be made available to users to emphasize the importance of adhering to the forecourt signage and mobile phone usage policy.

vi. **Reporting Violations:** Users witnessing any violations of the mobile phone usage policy should report them promptly to forecourt attendants or through designated reporting channels.

6.7.3 Hazardous Areas

Hazardous areas shall be clearly defined through signage, and guidelines shall be enforced to restrict device usage in these areas.

The use of electronic devices, including but not limited to mobile phones, is strictly prohibited within designated hazardous areas. Users must power off or stow their devices before entering these zones to minimize distractions and reduce the risk of accidents.

Individuals witnessing any violations of the hazardous area policies, including unauthorized device usage, should report them immediately to forecourt attendants.

6.8 Payment Processor

The Payment Processor plays a critical role in ensuring the smooth and secure processing of fuel payments by connecting the necessary payment networks and financial institutions involved in the transactions. Therefore, the selected Payment Processor shall comply with relevant regulations and industry standards.

Convenience Pay shall enter into a contract with the Payment Processor which shall include a clear and comprehensive Service Level Agreement (SLA) outlining the agreed-upon service levels, performance targets, and expectations, including but not limited to transaction processing time, system availability, Customer support response time, and any other relevant performance metrics.

The consequences of failing to meet the agreed-upon service levels shall also be clearly outlined.

6.9 Merchant/ Customer Experience

Convenience Pay shall prioritize the needs and concerns of all onboarded Merchants and Customers.

6.9.1 Transparency

i. Transparent and accurate information regarding pricing and fees associated with the app shall be provided to Merchants and Customers on the Convenience Pay website. This includes clearly communicating any transaction fees, or additional costs involved.

ii. Convenience Pay's Terms and Conditions shall be easily accessible to Merchants and Customers, outlining the rights, obligations, and responsibilities of both parties. These terms and conditions cover aspects such as data privacy, security measures, dispute resolution, and any other relevant contractual details. Merchants and Customers are required to review and understand the terms and conditions before using the application.

iii. Customers shall be provided with transparent and detailed transaction information, including the order summary and payment details, in order to confirm the transaction.

iv. Customers shall receive immediate confirmation of successful or failed transactions, including detailed transaction information.

6.9.2 Issues and Complaints

i. Multiple communication channels shall be offered for Merchants and Customers to reach out with questions, concerns, or feedback. These channels shall include email, online and telephone support.

ii. Merchant or Customer issues or complaints shall be addressed in a timely manner. The Customer service representative shall provide an initial response within a defined timeframe, acknowledging the receipt of the complaint and outlining the steps to be taken for resolution. The specific response time may vary depending on the nature and complexity of the issue. Once the resolution is implemented, the team shall follow up with the Merchant or Customer to ensure their satisfaction and confirm that the issue has been resolved to their expectation.

iii. Stakeholder insights and feedback shall be gathered through various channels, such as surveys, feedback forms, social media interactions, and support interactions to understand their evolving needs, preferences, and expectations. This information shall guide Convenience Pay's initiatives to align with Customer requirements.

iv. Customer support shall be promptly and professionally handled. Merchants shall be responsible for facilitating queries and resolution where applicable.

6.10 Fees

A clear and comprehensive fee structure shall be established for the services offered. The applicable fees, including transaction fees, or any other charges, shall be clearly communicated to Customers prior to utilizing the services.

Any changes to the fee structure shall also be communicated in advance to Customers, providing reasonable notice.

6.11 Policy Updates

This business policy is subject to periodic review and update as required. Stakeholders shall be notified of any significant changes to the policy, and their continued usage of the Automated Vehicle Fueling app will be considered acceptance of the revised policy.

7.0 RISK ANALYSIS

The following table summarizes the risks associated with this procedure and related controls to mitigate these risks.

No.	Identified Risk	Mitigative Control	Control Reference
1.	**Environmental and Safety Risks**		
1.1	*Customer Distraction* Customers using their mobile phones for purposes other than payment while fueling, leading to increased risk of spills and accidents due to reduced attention on the refueling task, resulting in potential damage to the environment, customer safety hazards, and reputational damage.	• Develop in-app safety guidelines emphasizing the importance of focusing on the refueling task. • Conduct staff training to observe and engage customers who are distracted using their mobile phone while fueling • Conduct public awareness campaigns to educate customers about safe mobile app usage. • Display clear forecourt signage illustrating the purpose of the mobile phone for payment and prohibiting usage while fueling at the dispenser • Regularly update safety measures and guidelines based on incident reports. • Collaborate with regulators, safety bodies and other stakeholders to improve safety practices. • Establish emergency procedures for quick response to incidents	6.7
1.2	*Mobile Phone Usage in Hazardous Areas* Customers using mobile devices in areas designated as hazardous during fueling, maintenance, or deliveries leading to increased risk of accidents posing severe safety and environmental risks, resulting in injury to Customers and staff, and damage to the service station and surrounding properties.	• Clearly define hazardous areas through signage with restricted device usage and enforce guidelines for safety in these areas. • Conduct regular staff and customer training regarding the dangers of using devices in hazardous zones	6.7.3

1.3	*Car Accidents* Customers attempting to use the mobile app while their vehicles are in motion leading to distracted driving and reduced focus on road safety, resulting in increased traffic accidents.	• Integrate technical features in the app to prevent usage when the vehicle is in motion. • Develop and implement clear user guidelines in the app specifying usage only when the vehicle is parked	6.7
1.4	*Ignition of Flammable Liquids or Vapors* The electronic nature of mobile phones can cause combustion of the device if something goes wrong, leading to the ignition of flammable vapors during the refueling process, resulting in incidents such as fires, or explosions.	• Prohibit phone usage at CNG dispensers or at hazardous areas • Install prominent signage at gas stations, clearly indicating the risks associated with electronic device usage during refueling • Provide clear guidelines on safe practices, including powering off and stowing devices before refueling	6.7
2.	**Legal and Regulatory Risks**		
2.2	*Compliance Violations:* Non-compliance with legal and regulatory requirements leading to penalties, legal actions, and service disruption, resulting in loss of Customer trust, financial losses, and reputational damage.	• Stay up-to-date on all relevant laws and regulations • Implement necessary safeguards for data protection • Assess and audit compliance with regulations periodically • Ensure that third-party service providers comply with relevant legal and regulatory requirements, industry standards, and best practices. Regularly review their compliance certifications and audit reports. • Engage in legal consultation to ensure app terms and conditions address liability and safety. • Collaborate with insurers to mitigate financial risks.	6.5

		• Strictly adhere to safety regulations to reduce the likelihood of legal issues	
3.	**IT/ Cyber Security Risks**		
3.1	*Security Breaches* Unauthorized access to sensitive customer data stored within the mobile app, leading to stolen payment credentials, unauthorized transactions, potential misuse of customer information for identity theft or financial fraud, resulting in financial losses for affected customers, reputational damage, legal consequences and customer attrition.	• Implement strong encryption protocols and data security measures for both data in transit and at rest. • Regularly conduct security audits and vulnerability assessments. • Educate employees on cybersecurity best practices and the importance of safeguarding customer data • Conduct penetration testing • Conduct periodic security audits and vulnerability scans • Implement fraud detection tools and mechanisms • Enforce strong authentication and verification protocols, such as passwords and OTPs • Monitor and analyze transaction patterns for suspicious activities • Comply with industry standards and regulatory requirements	6.5
3.2	*Security Breaches* Unauthorized interception of payment data during the communication between the mobile app and the dispenser system leading to compromised confidentiality and integrity of payment transactions resulting in financial losses for both customers and the fuel station and erosion of customer trust in the security of mobile payments.	• Implement secure communication channels, such as HTTPS, to prevent interception. • Utilize tokenization to protect sensitive payment information. • Update encryption protocols through the processor to address emerging threats	6.5.1
3.3	*Cybersecurity Threats:* The mobile app and automated systems may be vulnerable to hacking, data breaches, or other cyber-attacks, leading to unauthorized access to user	• Implement robust cybersecurity measures, encryption protocols, and regular security audits to safeguard user data and prevent unauthorized access.	6.5.4

	information, financial data, or even control of the fueling process.		
3.4	*System Failures and Technical Glitches* Unreliable service due to technical limitations or issues, system failures or glitches, leading to service disruptions, reversal of completed transactions, inconvenience for users and potential safety hazards, resulting in operational challenges, in managing and resolving transaction disputes, Customer frustration and attrition, loss of potential revenue, and damage to the Convenience Pay's and UNIPET's reputation	• Clearly define and communicate terms and conditions for mobile transactions. • Establish a responsive customer support system to address transaction-related concerns promptly. • Implement a transparent dispute resolution process with clear timelines and communication channels • Perform regular maintenance and updates • Ensure persons involved in building the test scenarios have a thorough understanding of the desired business solution, the software requirements, the process flows and the cultural and legal environment in which the solution will exist, to ensure that all possible scenarios are considered. • Conduct extensive and rigorous testing to ensure that the system works in all possible scenarios. Testing should include: 1. Stress testing to ensure system functions under a high volume of transactions. 2. Regression Testing, and 3. Functionality testing to ensure that the system functions as it should. Ensure that the testing process is iterative from unit to integration to regression, as problems encountered in units are fixed • Ensure that visual alerts clearly signal service interruptions, and provide clarification on whether the transaction failed, if the	6.2.3 and 6.9.2

		service interruption occurred during the transaction Develop and implement backup strategies and have contingency and disaster recovery plans in place.	
4.	**Operational Risks**		
4.1	*Operational Disruptions* Unplanned disruptions in the operation of the mobile payment or dispenser system leading to inconvenience to customers and potential dissatisfaction resulting in reputational damage and loss of potential revenue.	• Implement redundant systems and backup solutions to ensure continuous operation. • Schedule regular maintenance during off-peak hours to minimize impact. • Establish clear communication channels for customers to report issues and seek assistance	6.6 and 6.9.2
4.2	*System Incompatibility* Incompatibility between the mobile payment solution and dispenser systems, leading to transaction failures and potential customer frustration resulting in customer dissatisfaction and loss of revenue.	• Conduct thorough testing, including integration testing, before the full launch. • Implement a phased rollout to identify and resolve integration issues incrementally. • Establish a dedicated support team to assist customers during the initial implementation phase	6.2.2 and 6.2.3
4.3	*Fuel Theft* Unauthorized and fraudulent use of mobile payment solution for fuel purchases leading to financial losses for affected customers resulting in customer dissatisfaction and reputational and financial damage to the organization.	• Implement real-time transaction monitoring to detect and stop unusual activity. • Educate customers on safe mobile payment practices and regularly update them on security measures • Integrate a unique code into the app, after the purchase of fuel, that the Customer must enter at the pump in order to dispense the fuel.	6.3
5.	**Third Party Risks**		
5.1	*Payment Processor Risks* Relying on third-party payment processors for mobile transactions, which may face disruptions or security vulnerabilities leading to	• Conduct thorough due diligence when selecting third-party payment processors.	6.8

	transaction failures resulting in potential loss of revenue and erosion of customer trust and loyalty.	• Establish contingency plans and alternative providers to mitigate disruptions. • Monitor the performance and security practices of third-party processors regularly	
5.2	*Inadequate Selection of Payment Processor:* Data loss or corruption, leading to transaction errors, financial discrepancies and Customer dissatisfaction resulting in a failure to achieve financial targets and reputational damage.	• Ensure robust data backup and recovery mechanisms are implemented, which are regularly tested to ensure data integrity • Ensure redundancy measures are implemented to prevent single points of failure • Include these mitigants in the selection criteria for choosing a Payment Processor	6.5.1 and 6.5.2
5.3	*Issues with the Payment Options:* Technological instability leading to recurring service interruptions and technical problems, resulting in potential loss of business due to loss of confidence and reputational damage.	• Have clear service level agreements with the Payment Processor company, and enforce appropriate consequences for failing to meet service levels • Regularly assess the Payment Processor's performance and reliability	6.8
5.4	*Mobile Network Instability* Relying on mobile network providers for secure communication between the mobile app and dispenser, which may face outages or disruptions leading to inconvenience to customers and potential dissatisfaction resulting in erosion of customer trust and loyalty in the organization.	• Establish redundancy and failover mechanisms to mitigate the impact of network outages. • Collaborate with reliable mobile network providers with a strong track record of stability. • Communicate transparently with customers about potential network-related disruptions	6.6 and 6.9
6.	**Customer Service and Reputational Risks**		
6.1	*Inadequate Customer service* Inadequate Customer Service when calling in for support leading to Customer dissatisfaction, increased Customer complaints, negative online reviews, and loss of Customer loyalty, resulting in potential damage to the company's reputation and decreased business growth.	• Provide adequate training and resources to Customer service representatives to enable them to provide responsive and knowledgeable Customer support. • Address and resolve any issues or complaints promptly	6.9.2

		• Monitor Customer feedback and take corrective action if needed.	
6.2	*New Entrant* Hesitation and reluctancy of both Customers and Merchants to use the app, due to Convenience Pay's lack of industry experience, leading to limited or poor adoption of the service, low usage rates, limited revenue generation and decreasing Customer engagement, resulting in business objectives for the service not being met and potential setbacks in the organization's competitive position.	• Develop and implement targeted marketing and promotion strategies to raise awareness about the app, its benefits, and its competitive advantages. This can include content marketing, social media campaigns, and collaboration with industry influencers. • Communicate clearly the benefits and value of using the app to potential users, highlighting how it can simplify their payment processes, enhance security, or provide additional benefits • Update and enhance the app based on user feedback, technological advancements, and changing market needs. This demonstrates a commitment to ongoing improvement and encourages user adoption. • Provide incentives and attractive promotions as a new entrant attempting to attract Customers. • Ensure that the Sales Team is very experienced and works aggressively to capture market share. • Ensure Sales Team are incentivized to meet set sales targets. • Seek input from users and understand what features and functionality they will want.	6.9
6.3	*Poor Strategic Partnerships:* Strategic partnerships are developed with parties who are no longer interested, or who no longer exist, leading to Customers not accessing the products/services of	• Perform adequate and effective Market Research to identify potential strategic partners, such that ALL parties (Convenience Pay, the Strategic Partner, the	6.8

	the strategic partner, resulting in the strategic partner not realizing the promised benefits of the partnership.	Customer) benefit from the partnership. • Ensure that the agreement is well documented, and allows for ease of termination of the partnership, if necessary.	
6.4	*Customer Frustration* The time to fuel the vehicle elapses during refueling transactions, leading to delays in the refueling process, resulting in reputational damage and frustration among Customers waiting in line.	• Implement clear and timely notifications to alert users when the timer is about to expire. • Offer accessible customer support resources within the app, including real-time assistance for users experiencing timer-related issues.	6.2.1

8.0 REFERENCE DOCUMENTS AND RECORDS

No.	Name	Reference No.	Internal/ External	Retained By	Record Retention Period
1.	Convenience Pay Digital Wallet Policy	CPTL-DW-POL-0001	Internal	N/A	N/A
2.	Convenience Pay Digital Wallet Processes and Procedures	CPTL-DW-PRO-0001	Internal	N/A	N/A
3.	Convenience Pay Digital Wallet Terms of Use	CPTL-DWUA-0001	Internal	N/A	N/A

9.0 REVISON LOG

This Policy is reviewed to ensure its applicability and relevance to the systems and processes that it describes. A record of all amendments is recorded below:

No.	Page No.	Summary of Change	Approved By	Effective Date
1.	N/A	Initial release	Chief Executive Officer	31/Dec/2023