ŞARJAL TİCARET ŞİRKETİ LİMİTED

SECURITY POLICY

Get Energy

Effective date: 07 July 2026

Parameter	Details
Service Operator	ŞARJAL TİCARET ŞİRKETİ LİMİTED
Trading Name of the Service	Get Energy
Registration Number	MŞ28752
Company Electronic Number	102944933544
Address	Beşparmaklar Cad. Nazım Bodi Plaza No:4 Çatalköy Girne, TRNC
Website	getenergy.energy
E-mail	info@getenergy.energy

1. General Provisions

1.1. This Security Policy sets out the principal organisational, technical and procedural measures that ŞARJAL TİCARET ŞİRKETİ LİMİTED applies when providing the Get Energy service in order to protect users, payments, data, rental stations, equipment and the digital infrastructure of the service.

1.2. Get Energy enables users to rent portable charging devices through the website, a QR code, a payment page, a mobile application where available, and other digital channels supported by the Company. Basic rental may be carried out without mandatory account registration, unless registration or additional verification is expressly required for a specific transaction, security review, payment provider requirement or dispute resolution process.

1.3. This Policy forms part of the overall set of Get Energy legal documents and applies together with the Terms of Service, Privacy Policy, Rental Policy, Pricing Rules, Refund Policy, Payment and Automatic Charges Policy, Equipment Replacement Charge Policy and other service documents.

1.4. The purpose of this Policy is to explain to users and partners what security measures are applied when the service is used, what actions are expected from the user, and how the Company responds to threats, incidents, fraudulent actions, technical failures and attempts to misuse the service.

2. Scope of Application

2.1. This Policy applies to all digital and physical components of the Get Energy service, including the website, rental pages, payment pages, QR codes, rental stations, portable charging devices, internal administrative panels, technical support, payment processes and handling of user requests.

2.2. This Policy applies to users who start a rental through a QR code or website without mandatory registration, to users with an account, to employees and contractors of the Company, and to technical and payment providers involved in the provision of the service.

2.3. This Policy does not disclose internal technical details that could create a security risk for the service, including private keys, server configurations, internal addresses, login credentials, infrastructure administration procedures and other restricted-access information.

3. Core Security Principles

- lawfulness, transparency and proportionality of the security measures applied;
- minimisation of processed data and access rights;

- protection of payments and prevention of unauthorised transactions;
- segregation of access to administrative and technical functions;
- use of secure communication channels when data is transmitted;
- ongoing monitoring of rental stations and digital services;
- recording of significant technical events for the investigation of failures and disputes;
- timely response to incidents and user requests;
- maintaining a balance between convenient rental without registration and the necessary level of security.

3.2. The Company seeks to design the service so that a user can rent equipment quickly, while every action relating to payment, equipment release, return, equipment replacement charge or refund is technically confirmed and can be reviewed if a dispute arises.

4. Security of Rental Without Mandatory Registration

4.1. Web rental without mandatory registration means that a user may start a rental through a QR code, station page or payment page without first creating a permanent account. This model is used for user convenience and does not remove the need to accept the service legal documents before the rental starts.

4.2. Even where no account is created, the service may process technical and payment identifiers required to confirm the rental, link a specific transaction to specific equipment, process the return of equipment, calculate charges and protect against fraud.

4.3. The Company may request additional information, confirmation of a telephone number or e-mail address, payment verification or creation of an account if this is necessary for security, fraud prevention, dispute resolution, refund processing, investigation of non-returned equipment or compliance with payment organisation requirements.

4.4. The absence of mandatory registration does not mean that the payment transaction is anonymous. Payments may be processed by banks, payment systems, payment services and other settlement participants, which apply their own verification and security procedures.

5. Payment Security

5.1. Get Energy accepts payment through supported payment methods, including bank cards, Apple Pay, Google Pay and other methods available to the user at the time of payment. Payments are processed through payment providers, banks and payment organisations connected to the service.

5.2. The Company does not store the full bank card number, card security code or other full card details that are not required by the Company to provide the service. Full payment details are processed by the payment provider, bank or payment service applying its own payment data security standards.

5.3. For security purposes, a payment transaction may include pre-authorisation, temporary hold of funds, 3D Secure verification, confirmation through the user’s bank, tokenisation of the payment method, a retry of an unsuccessful payment, and other checks provided by the payment organisation.

5.4. When Apple Pay or Google Pay is used, the actual card details are generally replaced by a payment token, and transaction confirmation is performed by the payment service and the user’s device. The Company receives only the information required to confirm the transaction, perform the rental and resolve possible disputes.

Measure	Description
Payment confirmation	Verification of the payment transaction by the bank, payment provider or payment service before equipment is released.
Pre-authorisation	Temporary hold of an amount required to secure payment for the rental, possible subsequent charges or equipment replacement charge.
3D Secure	Additional transaction confirmation by the user through the bank or payment service, where such verification applies.
Payment token	A technical identifier of the payment method that allows subsequent charges under the rental terms without the Company storing full card details.
Payment retry	A repeated request to the payment provider where a transaction is unsuccessful, if permitted by the service rules and the payment organisation.

6. Security of QR Codes and Rental Pages

6.1. QR codes are used to connect the user to a specific station, station slot, rental page or payment page. The user should check that, after scanning the QR code, he or she is directed to a Get Energy page or another official payment channel indicated by the service.

6.2. The Company recommends not entering payment details on pages where the address appears suspicious, contains misspellings of the domain, does not use a secure connection or visually does not match the official service interface.

6.3. If the user discovers a damaged QR code sticker, a third-party code placed over the original code, a suspicious payment page or a message asking the user to pay outside the official Get Energy process, the user should stop the transaction and contact support.

6.4. The Company may block or temporarily disable QR codes, stations or individual slots if there are signs of substitution, technical malfunction, unauthorised interference or other security threats.

7. Security of Stations and Equipment

7.1. Get Energy stations are intended for automated release and return of portable charging devices. Each release and return operation may be recorded by the station’s technical systems, software and event logs.

7.2. Equipment may have unique identifiers that allow a specific device to be linked to a specific rental transaction, release station, return station, release time and return time.

7.3. The user must handle the station and equipment carefully, must not open the casing, alter the structure, remove identifiers, attempt to bypass the release or return mechanism, or perform actions that may compromise the security of the service.

7.4. If the equipment appears damaged, overheated, has signs of tampering, a burning smell, casing deformation, a damaged connector or any other obvious defect, the user must stop using it, return it to a station where this can be done safely and notify support.

7.5. The Company may temporarily block equipment or a station if signs of damage, incorrect return, technical error, fraud or a threat to user safety are detected.

8. Protection of Personal Data and Technical Data

8.1. The Company processes personal and technical data in accordance with the Privacy Policy. For security purposes, information about the payment, rental, station, equipment, browser, device, transaction time, technical errors, network events and user requests may be processed.

8.2. Security data is used to confirm transactions, prevent fraud, protect payments, investigate disputes, monitor service availability and comply with lawful requirements.

8.3. The Company applies the principle of minimisation: data is collected and stored only to the extent necessary for the relevant purpose. Access to data is granted only to persons and systems that need it to perform their work or contractual duties.

8.4. Data may be transferred to third parties only in the cases provided by the service legal documents, applicable law, the contract with the user, payment organisation requirements or lawful requests from competent authorities.

9. Secure Data Transmission

9.1. Secure communication channels, including HTTPS/TLS where supported by the relevant component of the service, are used to transmit data between the user, website, payment page and server infrastructure.

9.2. The user should not continue entering payment details if the browser warns about an insecure connection, invalid certificate, website substitution or other security risk.

9.3. The Company may restrict access from outdated, insecure or unsupported versions of browsers, devices, software or network clients if their use creates an increased risk for the service or users.

9.4. Transmission of internal data between service components may additionally be protected by access control measures, internal keys, network restrictions, logging and integrity controls.

10. Access Management

10.1. Access by employees, contractors and technical providers to Get Energy administrative systems is provided on a need-to-know basis and according to the principle of least privilege.

10.2. The Company may use individual accounts, role-based access control, action logging, functional access limits, periodic review of access rights and revocation of access after termination of cooperation or change of duties.

10.3. Access to payment operations, personal data, security logs, tariff settings, station management and refund operations must be limited to a restricted group of authorised persons.

10.4. Employees and contractors must maintain confidentiality, must not transfer credentials to third parties, must not use access outside legitimate work requirements and must promptly report suspicious events.

Principle	Practical meaning
Least privilege	Each internal system user receives only the rights required for his or her functions.
Segregation of duties	Payment, tariff, station and refund operations may be divided between different roles.
Logging	Significant actions in administrative systems may be recorded for control and investigation.
Access revocation	Access should be terminated upon dismissal, role change, contract completion or discovery of a breach.

11. Event Logs and Monitoring

11.1. To ensure security, the Company may maintain event logs relating to rentals, payments, equipment release and return, technical errors, actions in administrative systems, service requests and user support communications.

11.2. Event logs are used to diagnose errors, prevent fraud, confirm the fact of rental or return, investigate payment disputes, protect the rights of the Company and users, and comply with payment organisation and legal requirements.

11.3. Event logs are not intended for unjustified surveillance of the user. Their content is limited to information necessary for security and correct operation of the service.

11.4. Retention periods for logs are determined by the purposes of processing, legal requirements, possible payment dispute periods, accounting retention periods and the need to protect the Company's rights.

12. Prevention of Fraud and Misuse

12.1. The Company applies measures to detect and prevent fraud, service abuse, attempts not to pay for rentals, attempts to bypass automatic charges, QR code substitution, use of another person's payment method, damage to equipment or non-return of equipment.

12.2. Indicators of increased risk may include multiple unsuccessful payments, repeated use of disputed payment methods, frequent transactions followed by disputes, unusual rental attempts, interference with a station, suspicious conduct during equipment return or inconsistency in the technical data of a transaction.

12.3. If an increased risk is detected, the Company may refuse to release equipment, request additional confirmation, restrict access to the service, temporarily block the transaction, cancel the rental, transfer information to the payment provider or contact competent authorities where there are grounds to do so.

12.4. Security measures are applied proportionally to the nature of the risk and are not intended to unjustifiably restrict good-faith users.

13. Response to Security Incidents

13.1. A security incident means an event that may affect the confidentiality, integrity or availability of the service, payments, user data, stations, equipment or the Company's internal infrastructure.

13.2. Such events may include unauthorised access, payment page substitution, QR code substitution, mass technical errors, data leakage, malicious activity, station damage, unauthorised tariff changes, payment processing failure or another event involving material risk.

13.3. In the event of an incident, the Company may take measures including access restriction, disabling a station or page, temporary suspension of rentals, cancellation of suspicious transactions, notification of the payment provider, data restoration, log review, informing affected users and contacting competent authorities where necessary.

13.4. The Company's priority in incident response is the protection of users, payments, data, equipment and service resilience.

Stage	Content
Detection	Receipt of a signal from monitoring, a user request, a bank notice, a technical check or internal control.
Assessment	Determination of scale, affected transactions and possible impact on

	users and payments.
Containment	Restriction of access, disabling a problematic component, blocking a suspicious transaction or station.
Recovery	Return of the service to normal operation, verification of data integrity and correctness of payment operations.
Analysis	Review of root causes, adjustment of procedures, improvement of security measures and documentation of the result.

14. User Security Obligations

14.1. The user is responsible for the secure use of his or her device, browser, payment method, telephone number, e-mail address and other means used to interact with the service.

14.2. The user must:

- use only the official Get Energy website, official rental pages and payment pages;
- check the page address before entering payment details;
- not transfer to third parties data that allows control over a rental or payment;
- not use another person’s bank card or payment method without the owner’s permission;
- not attempt to bypass payment, temporary hold, automatic charge or the equipment return mechanism;
- promptly notify the Company about suspicious pages, fake QR codes, erroneous payments, malfunctioning stations or damaged equipment;
- return equipment to an operational station and check completion of the rental in the service interface, where this function is available.

14.3. If the user ignores obvious security warnings, enters data on a fake page, transfers a payment method to third parties or acts outside the service process, the Company may be limited in its ability to prevent losses or refund funds.

15. Official Communication Channels and Protection Against Fraudulent Messages

15.1. The official e-mail address for requests is info@getenergy.energy. The Company may additionally use other support channels indicated on the official website or in the service interface.

15.2. The Company should not request the full card number, card security code, bank application password, one-time bank code, e-mail login details or other information that would allow a third party to gain access to the user’s payment method.

15.3. The user should be cautious about messages offering payment through an external link, requesting a transfer to a personal account, asking for a confirmation code, asking the user to install an unknown application or to provide remote access to a device.

15.4. If a suspicious message is received, the user should stop interaction and forward the information to Get Energy support.

16. Loss or Compromise of the User’s Device

16.1. If the user loses a phone, bank card, device with access to a payment service, or suspects that third parties have obtained access to his or her payment method, the user must immediately contact the bank or payment service to block the payment method.

16.2. If the situation is connected to an active Get Energy rental, the user should notify the Company as soon as possible and provide available details of the rental: date, time, station, payment, transaction number, e-mail address or telephone number, where used.

16.3. The Company may take reasonable measures within its technical capabilities, including transaction review, restriction of further rental actions, assistance with completing the rental or transfer of information to the payment provider.

17. Backups and Recovery

17.1. The Company may use backups of data and settings required to restore service operation, confirm transactions, process payment disputes and refunds, and investigate technical errors.

17.2. Backups are protected according to their content and are used only for service recovery, business continuity, performance of legal obligations and protection of the rights of the Company and users.

17.3. Backup retention periods are determined by technical necessity, security requirements and the retention periods for the relevant data categories.

18. Security of Suppliers and Contractors

18.1. To provide the service, the Company may engage cloud infrastructure providers, payment providers, station maintenance contractors, developers, technical support services, accounting, legal and other professional advisers.

18.2. Suppliers and contractors must receive access only to the data and systems necessary to perform the relevant service. The Company may require them to maintain confidentiality and reasonable security measures.

18.3. Payment organisations and services involved in a transaction are also responsible, in their respective areas, for the security of payment processing, bank checks, 3D Secure confirmation and Apple Pay and Google Pay operations.

19. Limitations and No Absolute Guarantee

19.1. The Company applies reasonable security measures; however, no digital system, payment system, communication network, rental station or user device can be protected against all possible risks in an absolute manner.

19.2. The Company does not guarantee that the service will always operate without interruptions, errors, external failures, third-party actions, communication problems, bank delays or other circumstances outside the Company’s reasonable control.

19.3. If a security error, technical failure or payment issue affects a user, the Company will review the request under the relevant service documents, including the Refund Policy, Payment and Automatic Charges Policy and Complaint Handling Procedure.

20. Reporting Vulnerabilities and Suspicious Events

20.1. A user, partner or third party who discovers a potential vulnerability, QR code substitution, suspicious payment page, equipment release error, incorrect charge or another security issue may report it to info@getenergy.energy.

20.2. The report should preferably include the date and time of the event, page address, station number or location, description of the issue, screenshots where available, payment information without full card details, and contact details for feedback.

20.3. The reporting person must not use the discovered vulnerability to access other people's data, bypass payment, interfere with a station, obtain equipment without payment, disrupt the service or disclose restricted information.

21. Handling of Security Requests

21.1. Security requests are reviewed according to the nature of the event and its possible impact on the user, payments, equipment and the service. Priority is given to requests relating to payments, active rental, non-return of equipment, suspected fraud, data leakage or threats to user safety.

21.2. To review a request, the Company may ask for additional information required to identify the transaction, but it should not request the full card number, card security code, bank password or one-time confirmation code.

21.3. The outcome of a review may include a technical correction, refund or payment adjustment, blocking of a station or equipment, transfer of information to the payment provider, updating security procedures or another reasonable way to resolve the situation.

22. Changes to the Security Policy

22.1. The Company may amend this Security Policy if the service functionality, rental model, payment infrastructure, payment organisation requirements, technical security measures, legislation or internal Company procedures change.

22.2. The current version of the Policy is published on the Get Energy website. Continued use of the service after the new version enters into force means that the user has been informed of the updated terms to the extent applicable to the use of the service.

23. Contact Information

23.1. For questions related to security, suspicious messages, QR code substitution, payment risks, technical incidents and data protection, the user may contact Get Energy by e-mail at info@getenergy.energy.

23.2. When contacting the Company, the user should not send the full bank card number, card security code, bank password, one-time confirmation codes or other information that may allow third parties to make a payment transaction.

Appendix 1. Brief Rules for Safe Use of the Service

1. Scan the QR code only on a Get Energy station and check the page address before payment.

2. Do not enter payment details on pages that look suspicious or do not use a secure connection.

3. Do not disclose one-time bank codes or card details to anyone.

4. Do not use another person's payment method without the owner's permission.

5. Check that the equipment has actually been released by the station and that the rental has started correctly.

6. After returning the equipment, make sure that the rental is completed in the service interface, where this function is available.

7. Report a damaged station, fake QR code, erroneous charge or suspicious message to support.

8. Do not open the equipment, alter its structure or transfer it to third parties in circumvention of the rental terms.

9. If your phone or card is lost, immediately contact your bank or payment service.

10. Use only official Get Energy channels for support and payment.

Appendix 2. Matrix of Main Security Measures

Area	Main Measures
Payments	Payment providers, pre-authorisation, 3D Secure, tokenisation, bank checks.
QR codes	Linking to official pages, ability to block suspicious codes, monitoring of user reports.
Stations	Recording of release and return operations, disabling malfunctioning stations, review of disputed operations.
Equipment	Device identifiers, linking to the rental transaction, return rules and equipment replacement charge.
Data	Minimisation, access control, secure transmission, event logs.
User	Checking the page address, protecting the payment method, reporting suspicious events.
Support	Receiving requests, verifying transactions, interaction with payment organisations and technical teams.
Incidents	Detection, containment, recovery, root-cause analysis and improvement of procedures.

Appendix 3. Actions Prohibited for Security Purposes

For the protection of users, payments, stations, equipment and data, the following actions are prohibited. This list is not exhaustive; the Company may assess other actions as a security breach if they create a risk for the service, users, payments or equipment.

Prohibited Action	Description
QR code substitution	Placing another sticker over the official QR code, changing the code, redirecting the user to an external page or creating a similar payment page.
Payment bypass	Attempting to obtain equipment without confirmed payment, interfering with the pre-authorisation or automatic charging process.
Station interference	Opening the casing, damaging the lock, forcibly removing equipment, disconnecting power or otherwise interfering with station operation.
Equipment interference	Opening the casing, removing identifiers, changing the structure, replacing elements or attempting to conceal damage.
Use of another person’s payment method	Payment with another person’s card, payment service or banking instrument without that person’s consent.
False request	Providing false information about return, malfunction, payment, loss of equipment or disputed transaction.
Mass automated requests	Creating excessive load on the website, rental pages, payment pages or technical interfaces of the service.
Disruption of the service	Attempting to obtain unauthorised access, change rental data, tariffs, payment statuses or return records.

Appendix 4. Information the Company Does Not Request

To protect users against fraud, the Company draws attention to the fact that, during normal communication with Get Energy support, the user should not transfer information that allows third parties to control a bank account, card, payment service or personal account.

Information or Action	Explanation
Card security code	The Company does not request the three-digit or four-digit security code of a bank card.
One-time bank code	The Company does not request confirmation codes sent by a bank or payment service.
Bank password	The Company does not request the password for a banking application, online bank or payment service.
Full card number	For review of a request, the last digits of the card, transaction number or payment receipt details are usually sufficient without disclosing full card details.
Access to a device	The Company does not ask users to install remote access software in order to make a payment or receive a refund.
Payment to a personal account	The Company does not ask users to transfer rental payments to personal accounts of employees, representatives or third parties.

Final Provisions

This Security Policy enters into force on the date stated above and applies to all transactions carried out through the Get Energy service, unless otherwise provided by mandatory legal requirements, payment organisation rules or a separate written agreement with the user or partner.