transpack®

GLOBAL MOBILITY

Predio Goodpark - Nave 5.
Colectora Ruta 2 Km. 39,5 - Ing. Allan, Buenos Aires.
T: (5411) 3221 6900 - **F:** (5411) 3221 6901
info@transpack.com.ar - **www.transpackinternational.com**

Cybersecurity Policy

1. Purpose

The purpose of this policy is to establish guidelines and procedures to protect the organization's digital assets and confidential information against cyber threats, ensuring the integrity, confidentiality, and availability of data.

2. Scope

This policy applies to all employees, contractors, and third parties who access, use, or manage the organization's technological resources and information.

3. Responsibilities

- The executive management will be responsible for providing the necessary resources and support to implement and maintain this policy.

- The information security team will oversee and execute cybersecurity measures.

- All employees and stakeholders must comply with this policy and follow the established guidelines.

4. Protection of Digital Assets

- All computing devices and systems shall be protected with strong and regularly updated passwords.

- Antivirus and antispyware software will be implemented on all network devices.

- Firewalls and content filters will be used to protect against intrusions and malicious attacks.

- Data backups will be regularly performed and stored in secure off-site locations.

5. Access Management

- Access permissions will be assigned based on the principle of least privilege, limiting access only to individuals who need the information to perform their duties.

Predio Goodpark - Nave 5.
Colectora Ruta 2 Km. 39,5 - Ing. Allan, Buenos Aires.
T: (5411) 3221 6900 - **F:** (5411) 3221 6901
info@transpack.com.ar - **www.transpackinternational.com**

- An identity and access management process will be implemented to create, modify, and revoke user accounts as necessary.

6. Awareness and Training

- Cybersecurity training will be provided to all employees to increase awareness of threats and security best practices.

- Phishing simulations and other awareness activities will be conducted to educate employees on how to recognize and avoid cyber attacks.

7. Security Incidents

- An incident management process will be established to detect, investigate, and respond to potential security breaches.

- Security incidents will be promptly reported to the information security team so that appropriate corrective actions can be taken. 8. Review and Update

- This policy will be reviewed and updated regularly to reflect changes in technology and cyber threats.

- Periodic compliance reviews will be conducted to ensure that this policy is effectively implemented throughout the organization.