

Juegoalo.com – Information Security Policy

Version 1.0

Effective Date: May 2026

Introduction

At Juegoalo.com, information security is considered a critical part of maintaining a safe, reliable, and responsible online gaming operation.

The company is committed to protecting customer information, internal systems, operational data, and business processes against unauthorized access, misuse, disclosure, disruption, alteration, or destruction.

This policy summarizes the information security principles, controls, and operational practices currently implemented within Juegoalo.com, taking into account the company's business model, technological infrastructure, operational processes, and regulatory obligations.

1. Purpose

The purpose of this Information Security Policy is to establish the general principles and controls adopted by Juegoalo.com to safeguard information assets, maintain operational resilience, reduce security risks, and support compliance with applicable regulatory requirements.

2. Scope

This policy applies to:

- All employees, contractors, and third-party providers.
 - All systems, platforms, devices, applications, and operational environments used by Juegoalo.com.
 - All customer, financial, operational, and internal company information.
 - All remote and on-site work environments.
-

3. Governance and Responsibilities

Information security responsibilities are shared across management, operational teams, and technology personnel.

The Compliance Officer, Risk Team, and relevant IT personnel oversee the implementation and monitoring of security-related controls.

Management is responsible for ensuring that appropriate resources, procedures, and controls are maintained to support information security objectives.

Employees and contractors are expected to follow internal security procedures and report potential incidents or suspicious activity when identified.

4. Risk Management

Juegoalo.com applies a risk-based approach to information security.

Potential security risks are evaluated periodically based on operational needs, business impact, system exposure, and emerging threats.

The company considers risks including:

- Unauthorized access.
- Fraud and account compromise.
- Data leakage.
- Phishing attacks.
- Malware and ransomware.
- Service interruptions.
- Third-party provider risks.
- Human error and misuse of systems.

Where relevant risks are identified, mitigation measures and internal escalation procedures may be implemented.

5. Access Control

Access to systems and operational information is restricted based on business needs and role responsibilities.

User access is managed through authorized accounts and internal approval processes.

Access rights may be modified or revoked when employees change roles or leave the company.

Juegoalo.com uses Microsoft-based collaboration and operational tools, including Microsoft Teams, to support internal communication and operational activities.

The company may implement additional authentication and security controls where appropriate, including password policies and multi-factor authentication for sensitive systems.

6. Data Protection and Confidentiality

Juegalo.com handles customer and operational information confidentially.

The company takes reasonable technical and organizational measures to protect:

- Customer information.
- Transactional data.
- Internal business information.
- Financial and operational records.
- Compliance-related information.

Sensitive information is only accessible to authorized personnel with legitimate business needs.

Data retention practices are managed in accordance with operational and regulatory requirements.

7. System and Network Security

Juegalo.com maintains technical safeguards designed to protect systems and operational environments.

Security measures may include:

- Endpoint protection.
- Anti-malware controls.
- Access restrictions.
- Secure authentication processes.
- Monitoring of suspicious activity.
- Software and security updates.
- Controlled remote access.

The company works to maintain secure operational environments and reduce exposure to unauthorized access or operational disruption.

8. Third-Party Providers

Juegalo.com works with external providers that support operational, verification, payment, and technology-related services.

Third-party providers may include:

- Identity verification providers.
- Cloud or hosting services.
- Payment-related providers.
- Operational support vendors.

The company seeks to work with reputable providers and may assess operational and security considerations before or during vendor relationships.

Where relevant, providers are expected to maintain appropriate confidentiality and security standards.

9. Incident Response

Juegalo.com maintains internal procedures for responding to security incidents, operational disruptions, or suspicious activity.

Potential incidents may include:

- Unauthorized access attempts.
- Fraud-related events.
- System compromise.
- Data exposure.
- Service interruptions.
- Phishing or malware-related events.

Incidents are reviewed internally by the appropriate personnel depending on the nature and severity of the issue.

Where necessary, corrective actions, escalation measures, access restrictions, or remediation activities may be implemented.

Relevant incidents may be documented for operational and compliance purposes.

10. Business Continuity and Backups

Juegalo.com recognizes the importance of maintaining operational continuity and protecting critical business information.

The company maintains backup and recovery measures designed to support operational resilience and minimize disruption.

Backup procedures, restoration capabilities, and continuity measures may be reviewed periodically depending on operational requirements and system criticality.

11. Monitoring and Logging

Operational and security-related activities may be monitored and logged to support:

- Security investigations.
- Fraud prevention.
- Operational monitoring.
- Compliance reviews.
- Incident analysis.

Access to logs and monitoring information is restricted to authorized personnel.

12. Employee Awareness and Training

Juegalo.com promotes security awareness among employees and relevant personnel.

Employees involved in operational, customer-facing, compliance, or technology-related functions may receive periodic guidance or training regarding:

- Information security responsibilities.
 - Confidentiality obligations.
 - Fraud prevention.
 - Phishing awareness.
 - Acceptable use of company systems.
 - Reporting of suspicious activity.
-