TRYSQUAAD / Security Incident Response Policy

Effective as of May 31, 2025

DEFINITIONS.

- **TRYSQUAAD**: Refers to the digital platform operated and managed by BRINNEX LLC, which facilitates the management and organization of sports services and other events.

1. INTRODUCTION.

TRYSQUAAD is committed to protecting the information and critical infrastructure of our systems. This policy establishes the framework for an effective response to any security incident that may compromise the integrity, confidentiality, or availability of our information.

2. OBJECTIVE.

The objective of this policy is to ensure a rapid and organized response to security incidents, minimizing the impact on business operations and protecting our customers and partners from the effects of security breaches.

3. SCOPE.

This policy applies to all employees, contractors, and third parties who handle or have access to TRYSQUAAD's systems and data.

4. DEFINITION OF SECURITY INCIDENTS.

A security incident is any confirmed or suspected event that results in unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations.

5. RESPONSE PROCEDURE.

- **Detection and Identification**: Monitoring systems are configured to alert the security team as soon as a potential security incident is detected.

- **Classification and Escalation**: The incident will be classified by severity and escalated appropriately according to established procedures.

- **Containment**: Immediate measures will be taken to contain the incident and prevent further damage.

- **Eradication and Recovery**: Once the incident is contained, work will proceed to eliminate the root cause and restore systems to normal operation.

- **Post-Incident Analysis**: An analysis will be conducted to understand how the incident occurred, how it was handled, and how it can be prevented in the future.

6. COMMUNICATION.

- **Internal**: Internal communications will be handled by the security team to ensure that all relevant stakeholders are informed during and after the incident.

- **External**: External communications, especially those directed to clients or regulators, will be managed in accordance with applicable laws and regulations to ensure transparency and legal compliance.

7. TRAINING AND AWARENESS.

Regular training on incident response will be conducted for all relevant personnel to ensure they are prepared to respond appropriately to any security or data breach.

8. REVIEW AND IMPROVEMENTS.

This policy will be reviewed annually or following a significant incident to ensure it remains effective and relevant. Lessons learned from incidents will be used to improve the policy and procedures.

CONTACT US

If you have questions about our **Security Incident Response Policy**, please contact us through the means provided on our website, contact us at: INFO@TRYSQUAAD.com, or
BRINNEX LLC
Attn: Legal Department – Privacy
P.O. Box 2051 NW 112 AV. SUITE 114, MIAMI, FL 33172