CHARTER REFERENCE

For Approval By: Chief Information Officer (CIO)

Version: 1.0

1. Purpose & Mission Statement

At Falconi, our mission is to empower our NFL clients at every stage of their careers, offering guidance in providing excellent representation, strategic career development, and support on and off the field at every turn.

We help our clients navigate their high-profile status, their finances, and manage their endorsements.

Our purpose is to serve as a trusted partner to all our athletes. We are committed to maximizing our clients' potential through our world-class expertise in contract negotiations, marketing opportunities at a global scale, and one on one mentorship at the highest level. We aim to cultivate a role that extends far beyond the field. We want to protect, guide, and help our clients through every transition in their careers.

2. Scope

The Cybersecurity Program applies to:

- **Digital Asset Protection**
  - **Ensuring the security of our clients' personal, financial, and professional data across our platforms**
- **Risk Management**
  - **We need to identify and mitigate any cybersecurity threats that are unique to our industry, targeting our athletes with all devices and social media accounts**
- **24/7 Threat Monitoring**
  - **Offering 24/7 threat monitoring of all activity to detect and respond to unauthorized access and potential data breaches**
- **Education and Cybersecurity Awareness**

  - **Equipping our clients and our teams with knowledge and best practices to help our team avoid cyber threats at all times**

- **Incident Response**
  - **Providing rapid-response protocols for any data breaches, compromised accounts, and threats foreseen to minimize damage done to the company**

3. Authority

The cybersecurity team operates under the authority granted by executive leadership and reports functionally to the Chief Information Security Officer (CISO). The team is authorized to:

- **Access all necessary systems and logs for security monitoring**
- **Enforce cybersecurity policies and standards**
- **Conduct security assessments and audits**
- **Investigate and respond to a security incident**
- **Provide recommendations to mitigate identified risks**

4. Responsibilities

The cybersecurity program will

- **Develop and maintain the cybersecurity policy framework**
- **Conduct regular risk assessments and vulnerability scans**
- **Manage incident response and recovery procedures**
- **Provide employee security awareness training**
- **Monitor compliance with internal policies and external regulations (e.g., NIST, ISO, GDPR)**
- **Ensure business continuity and disaster recovery planning from a security perspective**

Signatures

Chief Information Security Officer (CISO)

Name:

Signature: _______________

Date: ___________________

Chief Information Officer (CIO)

Name: _____________________

Signature: ________________

Date: ___________________