Incident Response Team Version 1.0

Group	Role	Responsibilities
IT/Cybersecurity	Chief Information Security Officer (Severity Level: 4)	Provides executive-level oversight during critical incidents Defines the strategic response direction, ensures alignment with Falconi's risk management policies Authorizes major decisions such as external disclosures and law enforcement involvement
	Incident Response Manager (Lead)	Oversees all incident response efforts, coordinates team actions, and reports to executive leadership

FALCONI

security@falconi.com
220 Gardenpoint Plaza, Suite 205, Newark, NJ 0710
(973) 555-1490

IT/Cybersecurity	Lead Security Analyst	Conducts threat detection, logs analysis, and technical investigation Runs vulnerability scans and ensures proper logging **Incident Documentation:** Maintains detailed incident logs, timelines, actions taken, and prepares post-incident reports for review and audits.
	SOC Analyst (Tier 1, 2)	**Tier 1:** Monitors real-time alerts, follows playbook for basic triage, and escalates true incidents to the Tier 2 SOC or Lead Security Analyst **Tier 2:** Conducts in-depth analysis of escalated alerts, supports incident triage and containment activities

IT/Cybersecurity	Digital Forensics Investigator	Collects and analyzes digital evidence, preserves chain of custody, and identifies root causes and attackers Additionally responsible for quarantining appropriate devices
	System Administrator	Maintains and restores servers, endpoints, user accounts, and local infrastructure **Backup & Recovery**: Applies patches and restores data and systems from backups, ensures backups are clean and recent

FALCONI
SPORTS AGENCY
security@falconi.com
220 Gardenpoint Plaza, Suite 205, Newark, NJ 0710
(973) 555-1490

	Network Administrator	Secures and monitors routers, switches, and Wi-Fi networks Segments networks and responds to unauthorized traffic
Legal	Legal/Compliance Officer	Coordinates with internal departments and outside counsel
	Privacy Officer	Assesses whether personal or health data was exposed Guides compliance with privacy laws (e.g. GDPR, CCPA, HIPAA)

Communications	Head of External Communications	Manages all communications with media and all other entities not within Falconi Additionally responsible for communicating adequate processes and work being done to effectively and efficiently resolve the incident
	Head of Internal Communications	Manages all internal communications within Falconi Reviews and publishes all messaging to current Falconi employees about incident status, next steps, etc.
	Social Media Manager (Severity Level: 3, 4)	Cultivates postings and monitors all activity across all Falconi social media accounts Additionally responsible for all messages and press releases communicated with customers and the surrounding public about the status of Falconi's IR

Human Resources	HR Director	Handles internal investigations involving employees, coordinates disciplinary actions, and ensures confidentiality and legal compliance

FALCONI
SPORTS AGENCY
security@falconi.com
220 Gardenpoint Plaza, Suite 205, Newark, NJ 0710
(973) 555-1490

Appendix-B Incident Severity & Response Classification Matrix

Severity Level (Decreasing Level)	Typical Incident Characteristics	Example of Impact	Incident Response
4	Critical breach; widespread system compromise with; sensitive data breached	An enterprise-wide attack involving multiple departments that prevents access to systems and disrupts business operations. Access to or theft of proprietary data.	Activate full IRT. Contain and remove threat. Notify leadership and legal. Begin recovery, forensics, and external coordination. Prepare required notifications. Conduct post-incident review.
3	Targeted attack; limited system compromise	Employee computer or account with sensitive data access compromised physical theft of device, unprotected media, or hard copy data.	Activate full IRT. Isolate affected system(s), notify legal and IT leads, begin internal investigation and recovery.
2	Malware Infection: Minor data access leaked	Company communication resources (email, phone system, etc.) may be compromised during a severe incident.	Engage IRT lead. Scan and remove malware, restore affected services, monitor for signs of escalation.
1	Low Risk vulnerability	A minor software or configuration vulnerability is discovered that does not currently expose sensitive data or systems. No active exploitation detected. Routine business operations remain unaffected.	Investigate the issue. Patch vulnerability during next maintenance cycle; monitor for exploitation attempts.