Falconi®
Sports
Agency

Cybersecurity Framework Overview

Foundational Policies, Plans, and Technical Readiness

Presented by: Cyber Essentials Team
In collaboration with: Risk Management and Incident Response Teams

Table of Contents

FALCONI
SPORTS AGENCY

❑ Leadership and Staff

❑ Systems and Surroundings

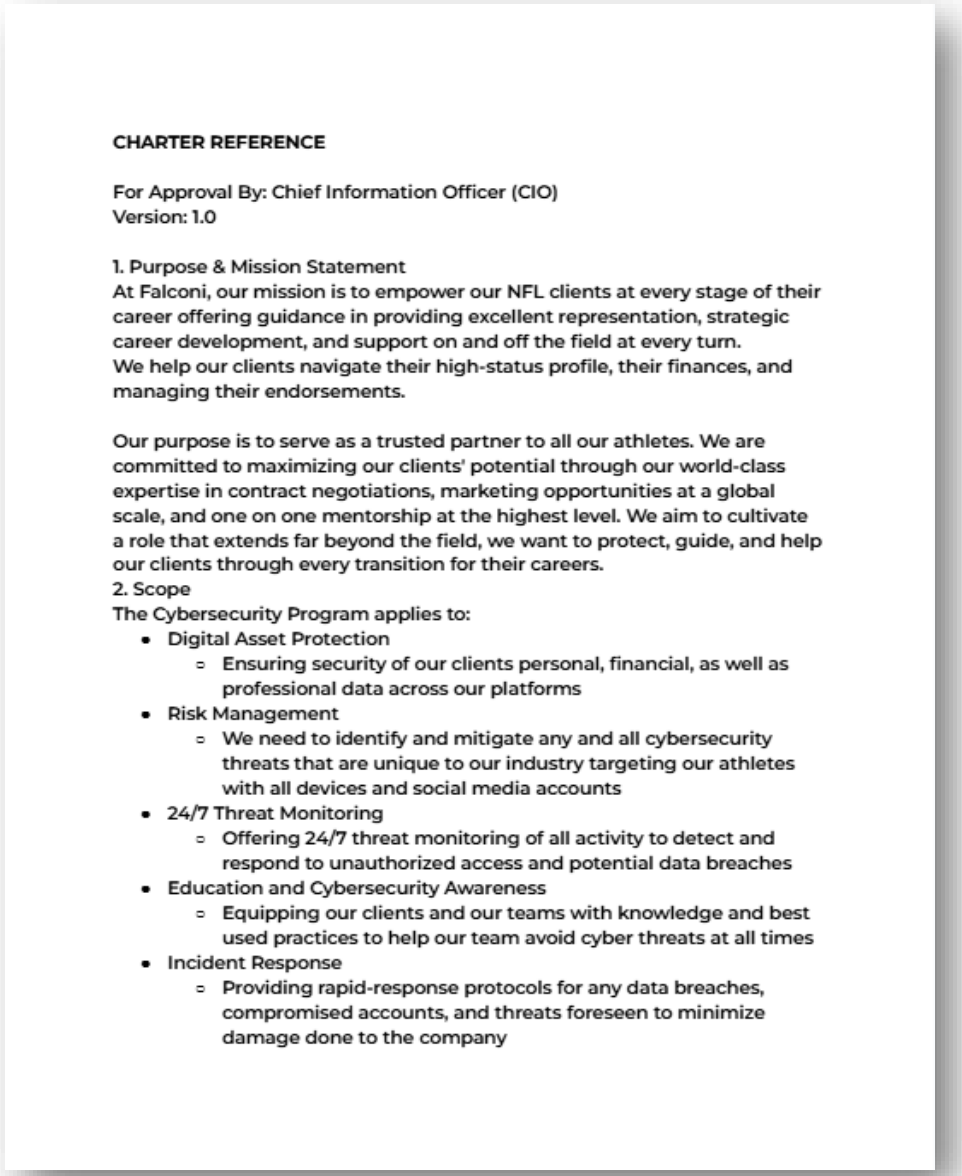
❑ Data and Crisis Response

FALCONI
SPORTS AGENCY

Leadership and Staff

Fostering Cybersecurity Culture & Developing Cybersecurity Awareness

Falconi Charter



CHARTER REFERENCE

For Approval By: Chief Information Officer (CIO)
Version: 1.0

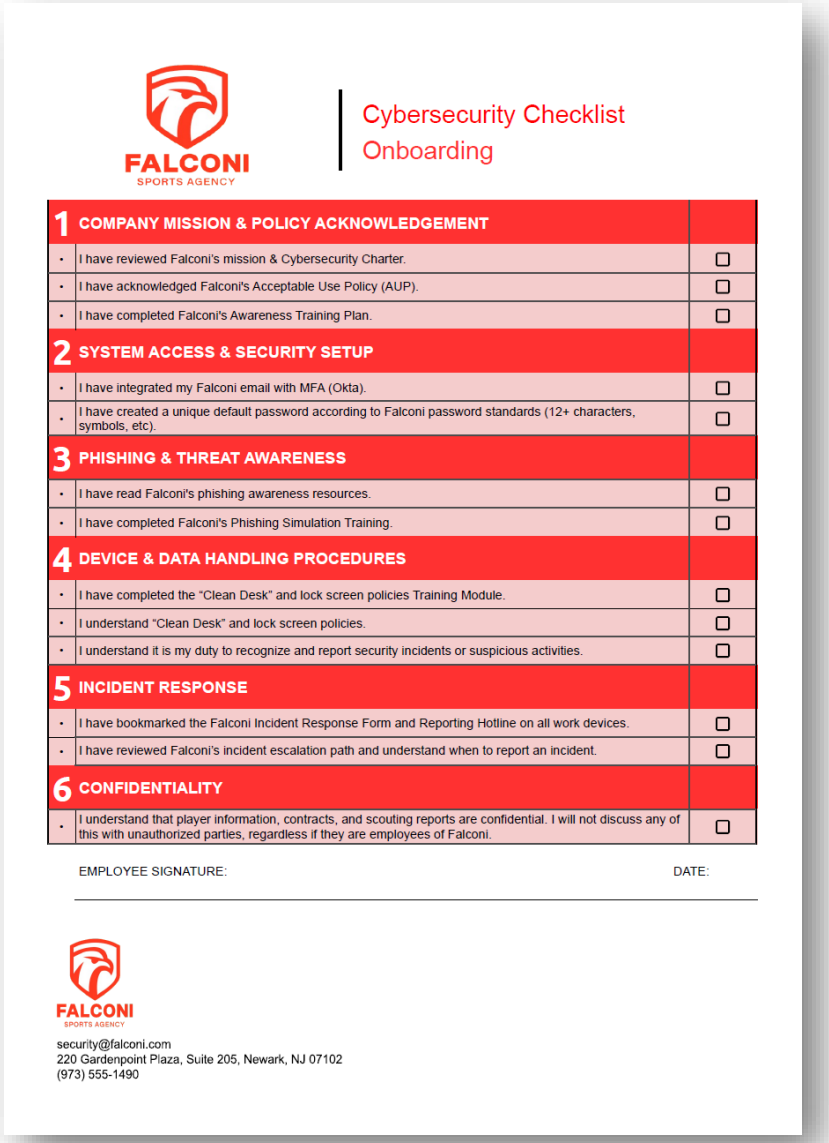
1. Purpose & Mission Statement
At Falconi, our mission is to empower our NFL clients at every stage of their career offering guidance in providing excellent representation, strategic career development, and support on and off the field at every turn.
We help our clients navigate their high-status profile, their finances, and managing 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 for their careers.
2. Scope
The Cybersecurity Program applies to:

- Digital Asset Protection
  - Ensuring security of our clients personal, financial, as well as professional data across our platforms
- Risk Management
  - We need to identify and mitigate any and all 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 used 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

- Purpose of the company
- Cybersecurity mission
- Staff acknowledgment
- Cyber readiness
- Risk assessments
- Awareness
- Compliance

Onboarding Checklist



FALCONI
SPORTS AGENCY

Cybersecurity Checklist
Onboarding

1	**COMPANY MISSION & POLICY ACKNOWLEDGEMENT**	
•	I have reviewed Falconi's mission & Cybersecurity Charter.	☐
•	I have acknowledged Falconi's Acceptable Use Policy (AUP).	☐
•	I have completed Falconi's Awareness Training Plan.	☐
2	**SYSTEM ACCESS & SECURITY SETUP**	
•	I have integrated my Falconi email with MFA (Okta).	☐
•	I have created a unique default password according to Falconi password standards (12+ characters, symbols, etc).	☐
3	**PHISHING & THREAT AWARENESS**	
•	I have read Falconi's phishing awareness resources.	☐
•	I have completed Falconi's Phishing Simulation Training.	☐
4	**DEVICE & DATA HANDLING PROCEDURES**	
•	I have completed the "Clean Desk" and lock screen policies Training Module.	☐
•	I understand "Clean Desk" and lock screen policies.	☐
•	I understand it is my duty to recognize and report security incidents or suspicious activities.	☐
5	**INCIDENT RESPONSE**	
•	I have bookmarked the Falconi Incident Response Form and Reporting Hotline on all work devices.	☐
•	I have reviewed Falconi's incident escalation path and understand when to report an incident.	☐
6	**CONFIDENTIALITY**	
•	I understand that player information, contracts, and scouting reports are confidential. I will not discuss any of this with unauthorized parties, regardless if they are employees of Falconi.	☐

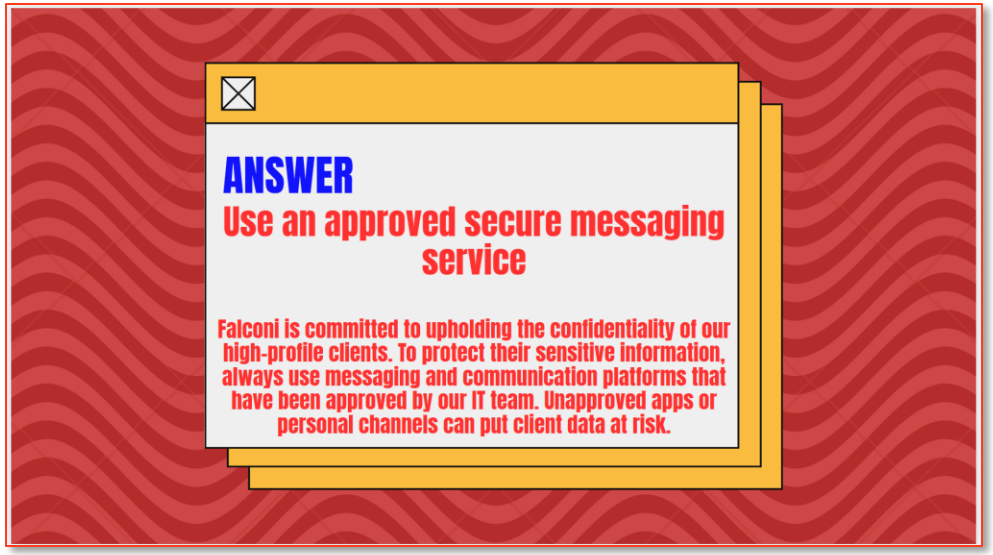
EMPLOYEE SIGNATURE: DATE:

FALCONI
SPORTS AGENCY

security@falconi.com
220 Gardenpoint Plaza, Suite 205, Newark, NJ 07102
(973) 555-1490

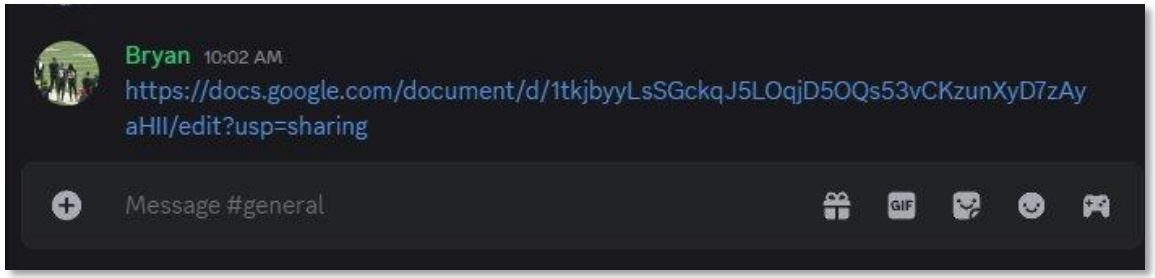
- Confirms awareness of cybersecurity mission
- Multi Factor Authentication
- Overall security
- Threat awareness
- Phishing readiness
- Protection of client data

Awareness Training Plan

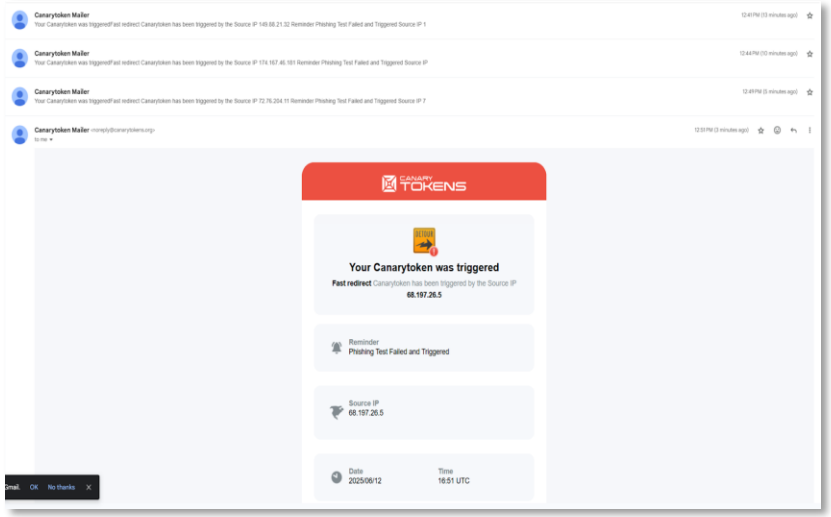


FALCONI
SPORTS AGENCY

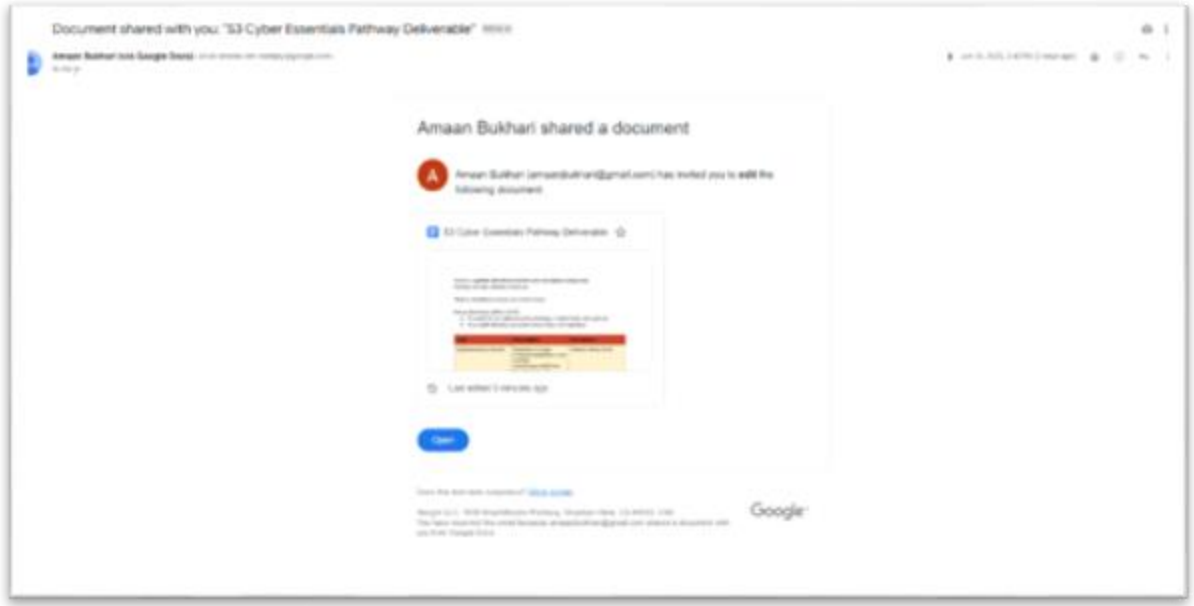
Phishing Training



Initial test



Link tracker



Final test

FALCONI
SPORTS AGENCY

System and Surroundings

Protecting Critical Assets & Managing Access Authorization

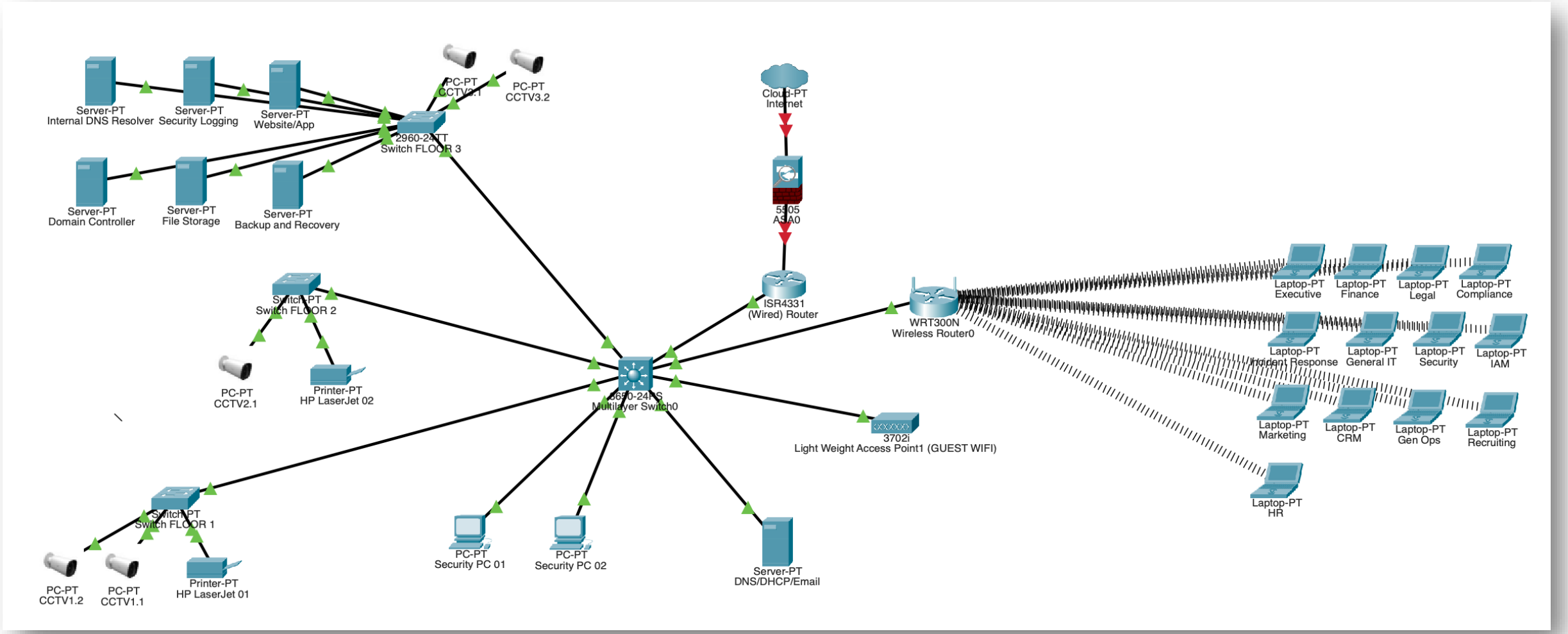
Asset Inventory

FALCONI
SPORTS AGENCY

Falconi Cybesecurity Asset Inventory Sheet										
Asset ID	Asset Name	Asset Type	Owner	Location	IP Address	OS/Firmware	Criticality	Licenses	Last License Renewal Date	Justification	Last Review Date
F01	Executive Laptop 01	Endpoints	Executive	HQ Floor 3	192.168.10.101	Windows Pro 11	Critical			Has access to all data from every department	2025-06-01
F02	Executive Laptop 02	Endpoints	Executive	HQ Floor 3	192.168.10.102	Windows Pro 11	Critical			Has access to all data from every department	2025-06-01
F03	Executive Laptop 03	Endpoints	Executive	HQ Floor 3	192.168.10.103	Windows Pro 11	Critical			Has access to all data from every department	2025-06-01
F04	Executive Laptop 04	Endpoints	Executive	HQ Floor 3	192.168.10.104	Windows Pro 11	Critical			Has access to all data from every department	2025-06-01
F05	Legal Laptop 01	Endpoints	Legal	HQ Floor 2	192.168.10.105	Windows Pro 11	Critical			Handles all legal contracts with/for clients	2025-06-01
F06	Legal Laptop 02	Endpoints	Legal	HQ Floor 2	192.168.10.106	Windows Pro 11	Critical			Handles all legal contracts with/for clients	2025-06-01
F07	Legal Laptop 03	Endpoints	Legal	HQ Floor 2	192.168.10.107	Windows Pro 11	Critical			Handles all legal contracts with/for clients	2025-06-01
F08	Finance Laptop 01	Endpoints	Fiancial	HQ Floor 2	192.168.10.108	Windows Pro 11	Critical			Handles payroll and access to financial data	2025-06-01
F34	Security Laptop 03	Endpoints	Security	SEC Floor 1	192.168.10.134	Windows Pro 11	High			Protectingthe Falconi staff, assets, information, and systems from threats, risks, and unauthorized access.	2025-06-01
F35	Security PC 01	Endpoints	Security	SEC Floor 1	192.168.10.135	Windows Pro 11	High			Protecting Falconi's staff , assets, information, and systems from threats, risks, and unauthorized access.	2025-06-01
F37	Security CCTV 01	Fixed	Security	SEC Floor 1	192.168.10.137	Windows Pro 11	High			Has access to all security cameras in SEC Building	2025-06-08
F38	Security CCTV 02	Fixed	Security	SEC Floor 2	192.168.10.138	Windows Pro 11	High			Has access to all security cameras in SEC building	2025-06-08
F39	HQ CCTV 01	Fixed	Security	HQ Floor 1	192.168.10.139	Windows Pro 11	High			Has access to all security cameras in HQ	2025-06-08
F40	HQ CCTV 02	Fixed	Security	HQ Floor 1	192.168.10.140	Windows Pro 11	High			Has access to all security cameras in HQ	2025-06-08
F45	HP LaserJet 02	Fixed	IT	HQ Floor 2	192.168.10.149	FutureSmart 5.7.1.2	Low			Monitors print jobs for each department and ensure efficient workflow for Falconi's business operations	2025-06-01
F46	Server - Domain Controller	IT Asset	IT	Network Room Floor 3	192.168.10.150	Windows Server	Critical	Windows Service License	2024-08-25	Provides authentication to manage user access for Falconi's network	2025-06-08
F47	Server - File Storage	IT Asset	IT	Network Room Floor 3	192.168.10.151	Windows Server	Critical	Windows OS License	2024-08-25	Ensure's secure and organized storage for critical files for Falconi's network	2025-06-08
F48	Server - Backup and Recovery	IT Asset	IT	Network Room Floor 3	192.168.10.152	Windows Server	Critical	Acronis Backup Software	2024-08-25	Protects data integrity by enabling regular backups and a strong recovery plan	2025-06-08
F49	Server - Website/App	IT Asset	IT	Network Room Floor 3	192.168.10.153	Windows Server	Critical	cPanel App License	2024-08-25	Host Falconi's services for internal and external users	2025-06-08
F50	Server - Security Logging (SIEM	IT Asset	IT	Network Room Floor 3	192.168.10.154	Linux	Critical	SIEM License	2024-08-25	Ensures detection and adequate response to threats	2025-06-08
F51	Server - Internal DNS Resolver	IT Asset	IT	Network Room Floor 3	192.168.10.155	Windows Server	Critical	Windows Server Licens	2024-08-25	Resolves internal hostnames, supports AD and logs	2025-06-08
F52	Switch FLOOR 1	Network	IT	HQ Floor 1	192.168.10.156	Cisco IOS 15.2(7)E4	High	Managed Switch License	Lifetime	Connects local devices (CCTV, printers, endpoints) on Floor 1	2025-06-08
F56	Router 01	Network	IT	Network Room Floor 1	192.168.10.1	IOS XE 16.12.4	Critical	CISCO IOS License	2024-08-25	Routes traffic between internal network and internet; gateway/firewall	2025-06-08
F60	Google Authenticator Software	Security Software	IT	Mobile Service	192.168.10.164	Android/iOS	High			2 Factor Authentication to verify user access	2025-06-01
F61	Google Workspace	SaaS	IT	Cloud Service	192.168.10.165	Google	Critical	Google Workspace Subscription	2024-08-25	Ensures collaboration, tasks, and organization efficiency across platform,	2025-06-01
F62	META Software	Web-based SaaS	IT	Web-based Service	192.168.10.166	Android/iOS/Any OS with browser	High	META SaaS Subscription	2024-08-25	Helps maintain, organize, protect, and portray a positive public image of Falconi and all our clients	2025-05-30
F63	CISCO Landline 01	Fixed	IT	HQ Floor 1	192.168.10.167	CUCM (Cisco Unified Communications Manager)	Medium			Provides staff a reliable form of communciation within Falconi and with clients	2025-06-10

Network Diagram

FALCONI
SPORTS AGENCY



Access Control

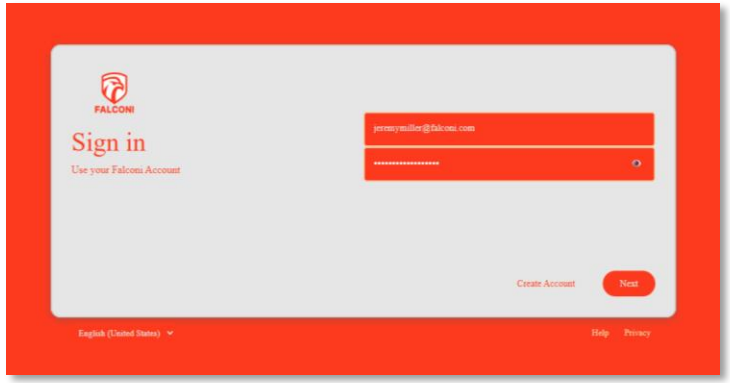
FALCONI
SPORTS AGENCY

	Software/IT				
Roles	Athelete Analytics Software	Google Workplace	Cloud Storage System	CRM Software	Inventory Tracker
CEO	N	RW	R	R	R
COO	N	RW	R	R	R
CISO	N	RW	RW	RW	R
CFO	N	RW	R	N	N
Legal Staff (legal counsel, contract attorney)	N	RW	N	N	N
Compliance Officer	R	RW	R	N	N
Payroll Manager	N	RW	N	N	N
Lead Recruiter	R	RW	R	N	N
Recruitment Analyst	RW	RW	R	R	N
HR Director	N	RW	R	N	N
IT Admin	RWX	RWX	RW	RWX	R
Network Analyst	N	RW	RW	R	R
Help Desk	N	RW	R	R	N
Analyst	R	RW	R	R	R
Analyst	R	RWX	RW	RW	R
Brand Manager	N	RW	N	N	N
Agent	R	RW	N	RW	N
Security Officer	N	RW	N	N	R
Terminated	N	N	N	N	N

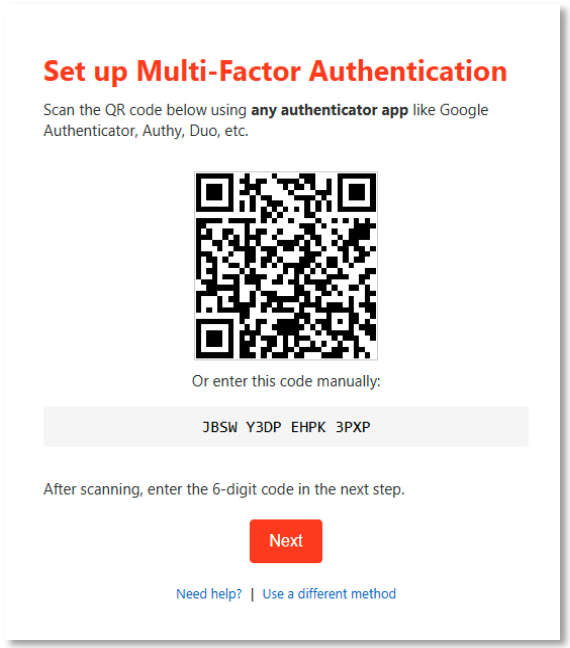
- Map legend
- Read, write, and executable
- Roles
- Knowledge on specific permissions

MFA Setup Guide

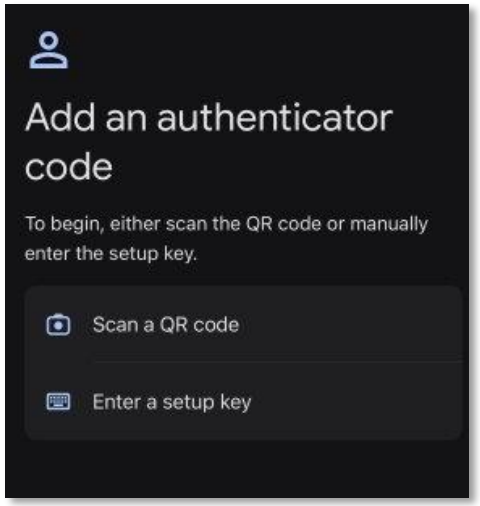
FALCONI
SPORTS AGENCY



User enters credentials



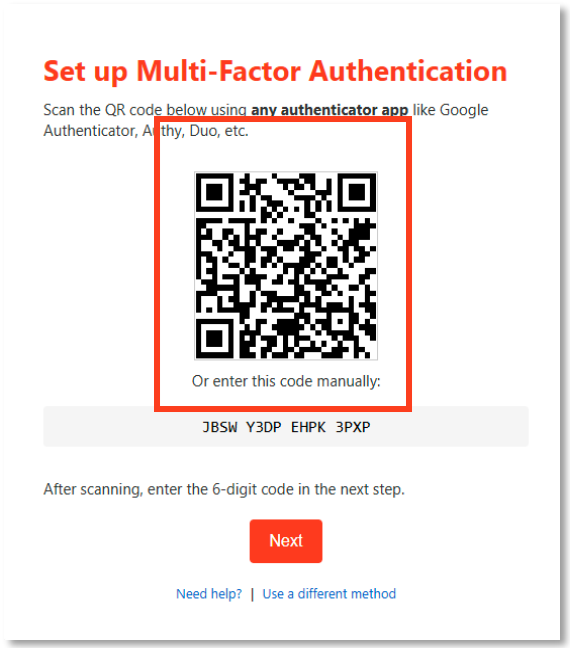
Prompted to setup MFA



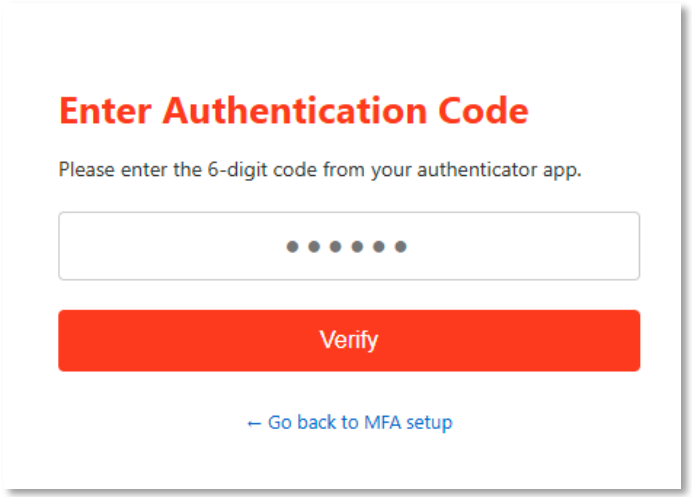
Add code on auth app

MFA Setup Guide (Cont.)

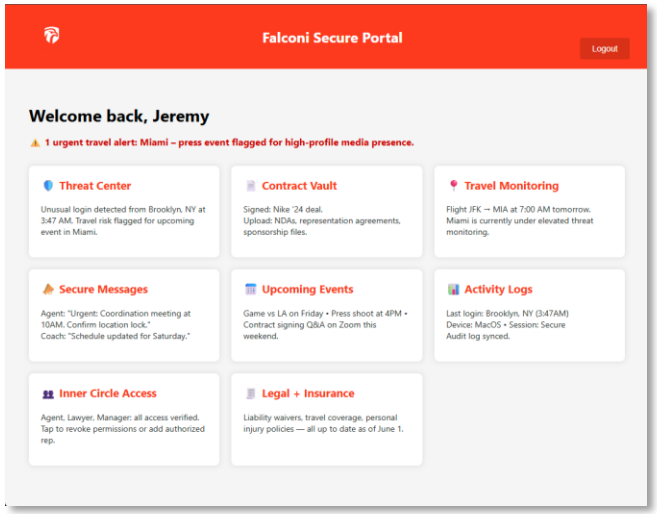
FALCONI
SPORTS AGENCY



Scan MFA code



Enter auth code



Access granted

FALCONI
SPORTS AGENCY

Data and Crisis Response

Protecting Data & Ensuring Operational Continuity

Data Classification

FALCONI
SPORTS AGENCY

Classification Level	Risk Level	Description	Access Rights	Breach Impact	Examples	Audit Controls	Storage Options	Security Measures	Compliance and Regulations
Public	Minimal risk	Data is not sensitive and can be shared publicly. Data will cause no harm to Falconi or its clients	No restrictions	No impact	• Publicly announced new clients	None Required	Public cloud storage or website CMS	Basic integrity checks and version control	None Required
Internal	Low risk	Data is intended for internal Falconi use only. Disclosure could cause operational or reputational harm.	Internal use only	Minor operational disruption	• Recruitment and signing procedures • Internal staff schedules • Staff contact directory • Internal memos • Falconi-Branded templates and digital assets	Log review (SIEM tools), Quarterly IT Audits	Internal file server or cloud platform with employee-only access	Password-protected access, endpoint security, logging	• Internal Policies • SPARTA (training materials)
Confidential	Medium risk	Sensitive data that should only be accessed on a need-to-know basis.	Restricted (need-to-know)	Moderate damage to business or reputation	• Onboarded 'pending' clients • Contracts in discussion • Draft offers • Athlete PII	Quarterly audits by governance board and data access reviews	Secure encrypted cloud drives or internal document management systems	Encryption (AES-256), access logs, MFA	• Internal Policies • SPARTA (FTC) • NFLPA Rules • CCPA (PII Baseline)
Restricted	High risk	Highly sensitive data with legal or financial consequences if disclosed.	Highly Restricted (need-to-know)	Severe impact including legal or financial penalties	• Athlete salaries • Athlete brand deal partnerships • Athlete health information • Athlete SPII	24/7 SIEM, real time alerts, monthly internal reviews, third-party audits	Encrypted storage on highly restricted cloud drives with access control	MFA, encryption at rest and transit, DLP tools	• Internal Policies • SPARTA (FTC) • NFLPA Rules • GDPR (Data Collection of European Residents) • HIPPA (not covered entity, but baseline) • CCPA (PII and SPII baseline)

Recovery Plan

FALCONI
SPORTS AGENCY

Data Category	Assets	Criticality	Frequency	Type
Employee	Employee Info	Moderate	Monthly/ Weekly	Full/ Incremental
	Employee Payroll	Moderate	Daily	Full
	Employee Contracts	Low	Weekly	Incremental
Client	Client Info	Critical	Daily	Full
	Client Finances	Critical	Daily	Full
	Client Contracts	Critical	Weekly	Differential
	CRM	Critical	Daily	Full
	Athlete Analytics Software	High	Weekly	Incremental
Business Operations	Endorsement obligations	Moderate	Weekly	Incremental
	Marketing outreach/social media	Moderate	Weekly	Incremental
	Internal Communication	High	Daily	Incremental
	Inventory List	Low	Weekly	Differential
Security & Network	Access Logs	High	Daily	Incremental
	Google Workspace	High	Daily	Full
	Surveillance System	Moderate	Weekly	Incremental
	Server - Domain Controller	Critical	Daily	Incremental
	Server - File Storage	High	Daily	Incremental
	Server - Website/App	High	Daily	Incremental
	Server - Security Logging (SIEM)	Critical	Daily	Full
	Server - Internal DNS Resolver	Moderate	Monthly	Incremental

Data backup plan

Data Category	Assets	Retention Period
Employee	PII	5 years
	Payroll	7 years
	Contracts	7 years
Client	Client PII	3 years after contract ends
	Client Finances	7 years
	Client Contracts	7 years
Business Operations	CRM	2 years
	Athlete Analytics Software	3 years
	Endorsement Obligations	4 years
	Marketing Outreach/Social Media	3 years
	Internal Communication	2 years
	Inventory List	2 years
Security & Compliance	Access Logs	1 year
	Surveillance System	60 days (unless an incident occurred)

Data retention policy

A. Local Backup:

- Provider: Network Attached Storage (NAS)
- Method: All assets listed are backed up daily or weekly per criticality.
- Retention: 90 days (about 3 months)
- Encryption: AES-256 encryption

B. Cloud Backup:

- Provider: Google Drive
- Frequency: Daily sync for essential files, weekly full backup
- Retention: 180 days (about 6 months)
- Encryption: TLS in transit, AES-256 encryption

C. Offsite Backup:

- Provider: Secure offsite facility
- Frequency: Monthly encrypted transfer of full back up images from the NAS
- Retention: 365 days (about 12 months)
- Encryption: AES-256 encryption

Backup strategy

Recovery Plan

FALCONI
SPORTS AGENCY

- **Recovery Time Objective (RTO):**
  - Critical Assets: < 3 hours
  - High Assets: < 6 hours
  - Moderate Assets: < 12 hours
  - Low Assets: < 24 hours
- **Recovery Point Objective (RPO):**
  - All Assets: < 24 hours

Recovery objective

- **Recovery Procedure:**
  - Identify the Issue:
    - The IT department identifies the nature of the incident.
    - Affected systems or accounts are isolated to prevent further damage.
  - Choose Backup Source:
    - Use local backup for quick recovery.
    - Use cloud backup if the local copy is unavailable.
    - Use offsite backup in cases of ransomware, disasters, or full system failures.
  - Restore Data
    - Restore individual files or full systems depending on the issue.
    - Prioritize critical data for faster recovery.
  - Check Everything
    - Ensure restored data functions properly.
    - Each department confirms that files and systems are working as expected. If any discrepancies are found, they should report to the IT admin for immediate action.
  - Document and Improve
    - Document the incident and how it was resolved.
    - Review the response and update the recovery plan after each major incident or test.

Recovery procedure

Role	Responsibility
CEO	Communicate with stakeholders regarding current status and updates
CISO	Oversee backup strategy, access permissions, ensure encryption and compliance
COO	Approves backup strategy plan and budget
Legal counsel	Draft the legal response plan and ensures compliance with applicable regulations in the event of a data breach
Compliance Officer	Ensure backup strategy meets regulatory requirements (NFLPA, data retention laws, HIPPA)
IT Admin	Manages backup configurations and scheduling
Network Analyst	Monitors cloud sync, storage limits, and encryption protocols
Employees	Save all work-related documents in approved folders or drives linked to backup systems. Avoid storing important files locally or in personal cloud accounts.

Roles and responsibilities

Recapitulation and Acknowledgments

FALCONI
SPORTS AGENCY

✓ Leadership and Staff

- Falconi Charter
- Onboarding Checklist
- Awareness Training Plan
- Phishing Simulation Development and Execution Summary

✓ Systems and Surroundings

- Asset Inventory
- Network Diagram
- Access Control Plan
- Multi Factor Authentication Simulation

✓ Data and Crisis Response

- Data Classification Policy
- Recovery Plan

Thanks to the following teams for their contributions:

- Risk Management: Onboarding Checklist, Access Control Plan, Data Classification Policy

- Incident Response: Awareness Training Plan, Network Diagram, Recovery Plan

Special thanks to our partners at Solutions³ LLC Mike Battistella, Kristen Nova, Shannon Conley, and Mark Marino!

What's next for Falconi® Sports Agency?

Monitoring and improving our Cyber awareness culture

Expansion past NFL (MLB, NBA, NHL, MLS)

Collaboration with universities and high schools for future athletes