Access Control Policy

Version 1.0

June 19th, 2025

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

Document Revision History

Date	Version	Description	Author
6/19/2025	1.0	Falconi Sports Agency Access Control Policy	CISO

Table of Contents

1. INTRODUCTION

Falconi Sports Agency has developed corporate policies that identify the security requirements for its information systems and personnel to ensure the integrity, confidentiality, and availability of its information. These policies are set forth by Falconi management and are in compliance with the Access Control family of controls found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5.

2. PURPOSE

This document outlines Falconi's Role-Based Access Control (RBAC) policy to ensure that users have access only to the data and systems necessary to perform their job functions, in alignment with the principle of least privilege. These policies are consistent with applicable state and federal laws, Executive Orders, directives, regulations, standards, and guidance.

3. SCOPE

The provisions of these policies pertain to all Falconi employees, contractors, third parties, and others who have access to company and client confidential information within Falconi systems and facilities.

4. KEY TERMS

Role-Based Access Control	A security model that restricts system access based on a user's role within the organization. Each role has specific permissions assigned to it.

Principle of Least Privilege	A cybersecurity best practice where users are granted the minimum levels of access needed to perform their responsibilities.
Access Type:	• R (Read): View access only. • RW (Read/Write): View and modify content. • RWX (Read/Write/Execute): Full admin-level access including execution or configuration rights. • RX (Read/Execute): Can view and run functions but not modify. • N (No Access): No permission to view or interact with the resource.
Sensitive Systems	Systems that handle confidential or critical data, such as employee payroll, client contracts, player financials, or Falconi's surveillance platforms. These require stricter access controls and monitoring.
Unauthorized Access	Any access to systems, data, or resources that is not explicitly permitted by the user’s role or assigned privileges. This includes both accidental and intentional violations.

5. ROLES AND RESPONSIBILITIES

These policies apply to all Falconi employees, contractors, business partners, third parties, and others who need or have access to Falconi systems and our clients' confidential information.

Group	Role	Access
Executive	CEO	Read-only access to payroll, contracts, client data, and finances; limited write access.
	COO	Read/write access to employee info, client info, contracts, and cloud storage.
	CISO	Read/write access primarily to security systems, dashboards, and incident response.
	CFO	Read/write access to payroll, financial data, and endorsement obligations.
Legal	Legal Counsel	Read/write access to employee contracts and player finances.
	Contract Attorney	Read/write access to legal documents, client contracts, and compliance records.

	Compliance Officer	Read/write access to compliance documents and contracts.
Finances	Payroll Manager	Read/write access to payroll systems and records.
Recruitment	Lead Recruiter	Read/write access to recruitment databases and player finances.
	Recruitment Analyst	Read/write access to client contracts, cloud, CRM, and analytics.
Human Resources	HR Director	Full read/write access to employee payroll, contracts, and personal info.
IT Department	IT Admin	Extensive read/write access to internal systems, databases, and cloud storage. Admin privileges to create, delete, or update access.
	Network Analyst	Read/write access to network configurations and analytics software.
	Help Desk	Read/write access to IT support systems, basic employee data, and internal technical documentation.

Cybersecurity	Risk Management Analyst	Primarily read and write access to security monitoring tools.
	Incident Response Analyst	Extensive read/write access to incident response and security logs.
Media & Marketing	Brand Manager	Read/write access to social media accounts and marketing content.
General Operations	Agent	Read/write access to client info, endorsements, contracts, and CRM.
	Security Officer	Read-only access to surveillance systems and physical access logs; minimal or no writing permissions.
Other	Promoted	Access is updated to match their new role.
	Temporary (Contracts, Interns, etc.)	Limited access based on their assigned group.
	Terminated	No access.

6. MANAGEMENT COMMITMENT

Falconi and its management are fully committed to protecting the confidentiality, integrity, and availability of corporate proprietary and production systems, facilities, and data, and ensuring the continuous availability of services in the Falconi system by implementing robust security controls.

7. COMPLIANCE

Compliance with these policies is mandatory. Falconi's policy requires that production systems meet or exceed the outlined requirements. The Information Owner will periodically assess compliance with these policies through an independent audit performed annually by an external vendor to identify non-compliance areas. Any findings from the audit will be remedied according to the auditing team's recommendations.

8. ACKNOWLEDGMENT

- All access to sensitive systems will be logged and monitored in real-time using security tools. The Risk Management Analysis team will review access logs biweekly to identify and investigate unauthorized access attempts.
- If an employee discovers that they have been granted unauthorized or excessive access privileges, they are required to notify the IT department immediately so that access levels can be corrected.
- Any suspected or confirmed unauthorized access attempts must be reported to the IT within 24 hours and will be subject to immediate investigation.
- Remote access to Falconi systems is only permitted when the employee is using a company-issued laptop, and multi-factor authentication (MFA) is enabled.
- Accessing Falconi's systems from personal devices is strictly prohibited, unless otherwise approved, and MFA is enabled.
- Upon termination of employment, the individual must return all Falconi-owned equipment, identification badges, documents (physical and digital), and any other work-related materials within five (5) business days. All system access rights and privileges will be revoked immediately upon termination to maintain the integrity and security of Falconi's data and systems.
- Upon promotion of employment, the individual must return all non-essential Falconi-owned technology and work-related materials. Previous access rights and privileges will be updated by the IT department to correctly match current access rights. Any new essential technology or work-related materials will be provided by their immediate supervisor.
- All temporary Falconi employees will be provided with limited access based on their assigned department. The access will be provided and monitored by the IT department.
- Failure to comply with this policy may result in disciplinary action, including termination and legal consequences.

□ By acknowledging this policy, you agree to adhere to the security protocols and responsibilities outlined above.

Name Date

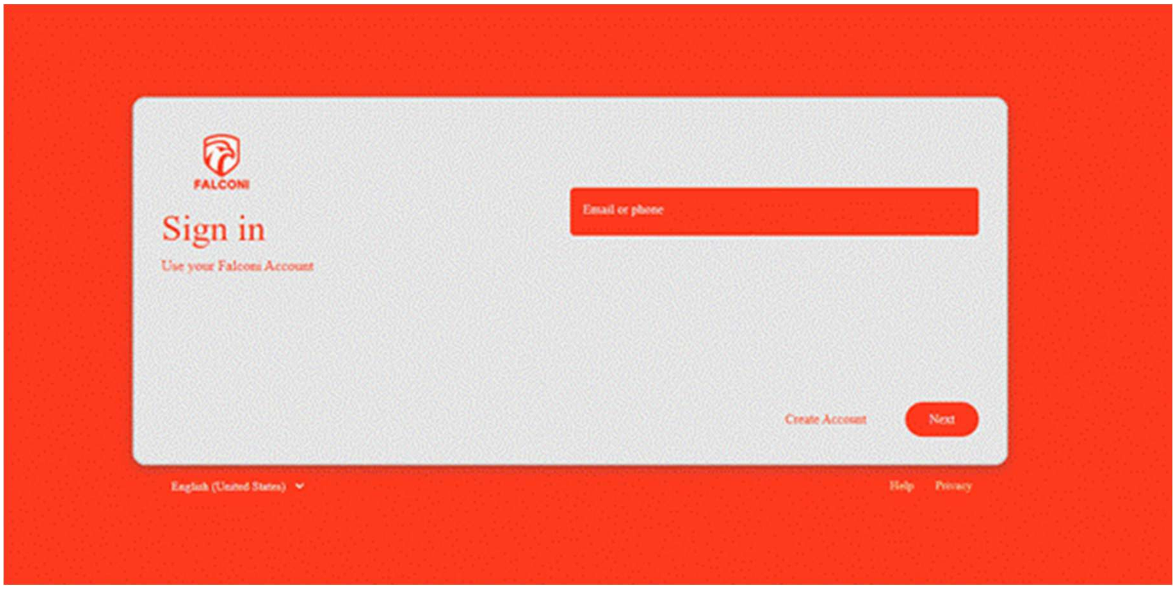
LINKED RESOURCES:

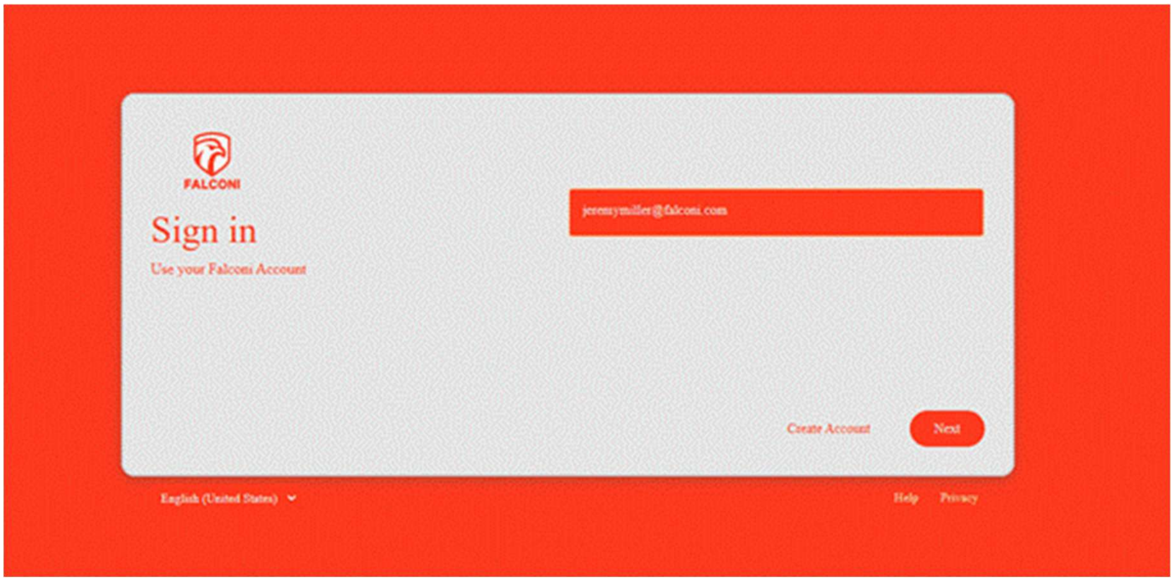
Document Name	Link
Falconi’s Criteria & Inventory Sheet	Cybersecurity Asset Inventory Sheet
Falconi’s Network Diagram	Network Infrastructure Diagram
Falconi’s Role Based Access Control Matrix	RBAC Matrix

Multi-Factor Authentication (MFA) Setup Guide

Step 1: Sign into the Falconi Portal

- The user enters their email or phone on the login screen

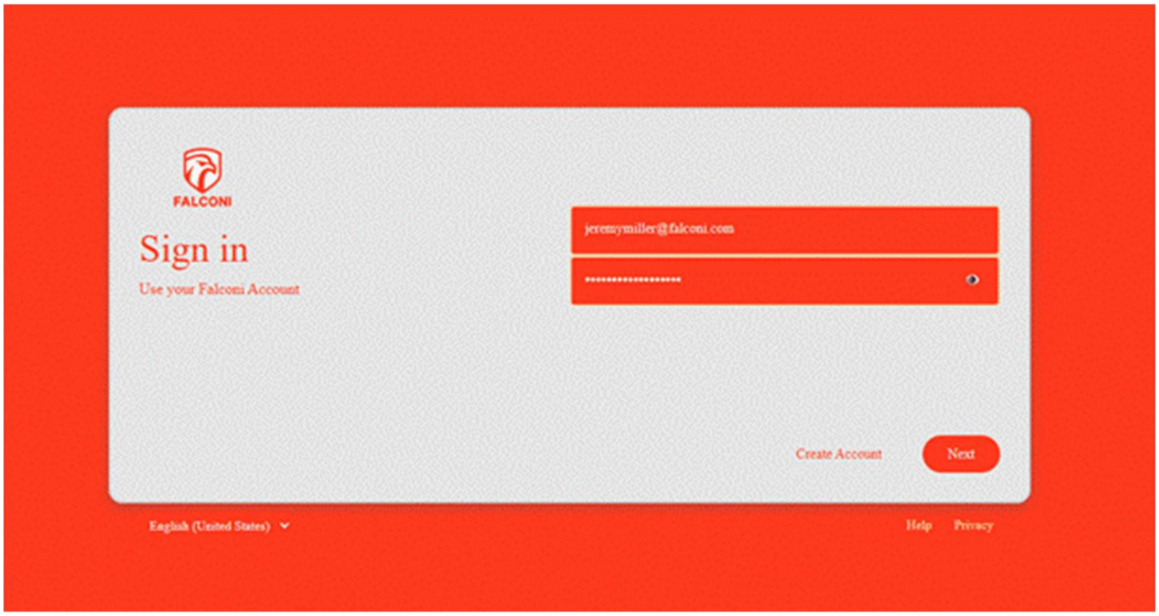




jeremymiller@falconi.com

Step 2: Enter Password

- The user types their Falconi account password



FALCONI

Sign in

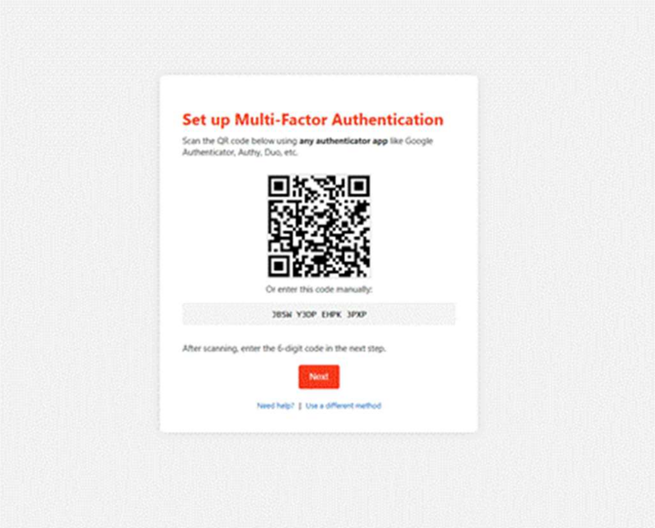
Use your Falconi Account

jeremymiller@falconi.com

•••••••••••••••••••

Step 3: Set up MFA with an Authenticator App

- The user is prompted to scan a QR code or manually enter a setup key using any MFA app like Google Authenticator, Authy, or Duo



Set up Multi-Factor Authentication

Scan the QR code below using **any authenticator app** like Google Authenticator, Authy, Duo, etc.

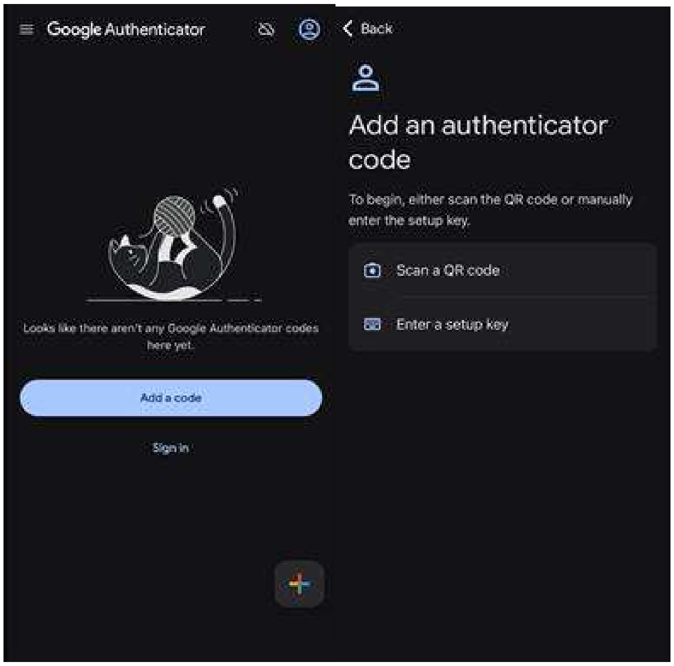
Or enter this code manually:

JBSW Y3DP EHPK 3PXP

After scanning, enter the 6-digit code in the next step.

Step 4: Scan QR Code Using Mobile Authenticator

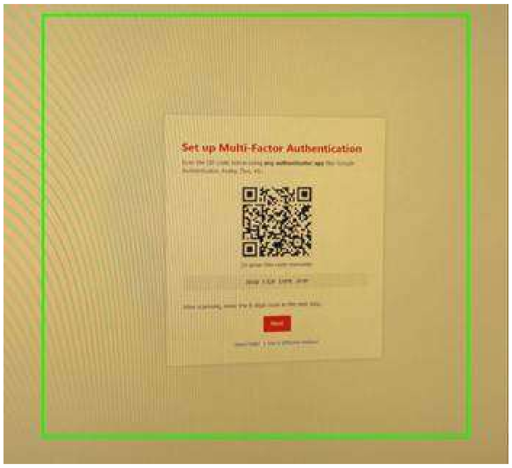
- On the user’s phone:
  1. Open the Authenticator app (Google in our example)
  2. Tap “Add a Code” → Scan QR Code
  3. Point the camera at the Falconi QR setup screen



Looks like there aren't any Google Authenticator codes here yet.

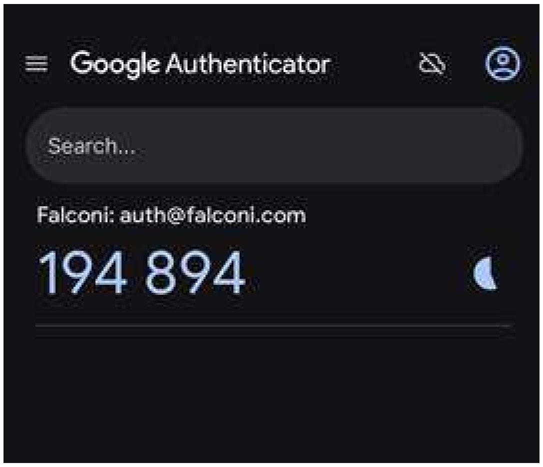
Add an authenticator code

To begin, either scan the QR code or manually enter the setup key.



Step 5: Code Is Now Stored in the App

- A 6-digit code is generated and refreshed every 30 seconds.
- This code is tied to this device only.

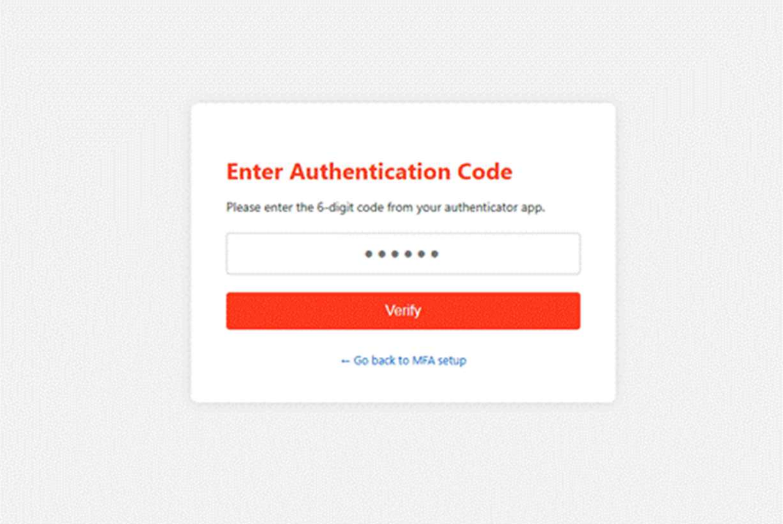


Falconi: auth@falconi.com

194 894

Step 6: Enter the 6-Digit Code

- Back on the Falconi portal, the user enters the 6-digit code from their authenticator.



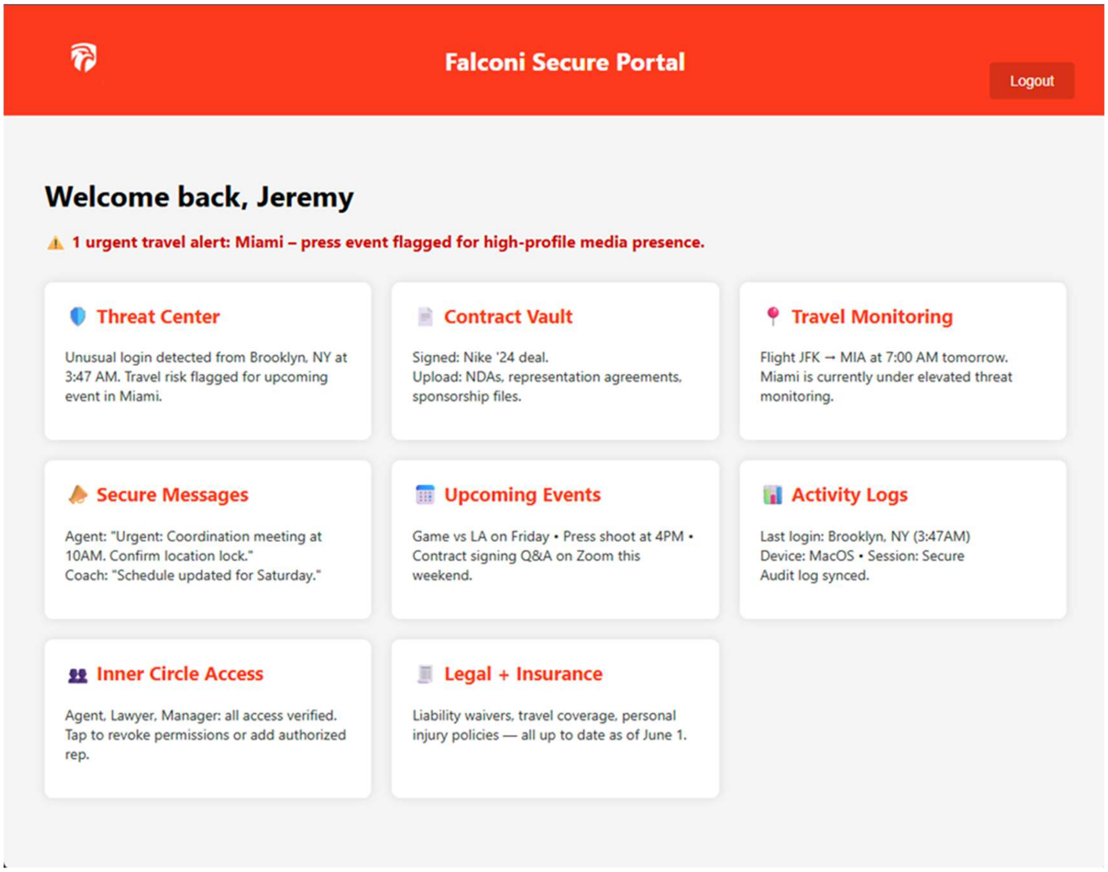
Enter Authentication Code

Please enter the 6-digit code from your authenticator app.

••••••

Step 7: Secure Access Granted

- Upon successful verification, the user is granted access to their secure Falconi account.



Welcome back, Jeremy

⚠ 1 urgent travel alert: Miami – press event flagged for high-profile media presence.

Threat Center
Unusual login detected from Brooklyn, NY at 3:47 AM. Travel risk flagged for upcoming event in Miami.

Contract Vault
Signed: Nike '24 deal.
Upload: NDAs, representation agreements, sponsorship files.

Travel Monitoring
Flight JFK → MIA at 7:00 AM tomorrow. Miami is currently under elevated threat monitoring.

Secure Messages
Agent: "Urgent: Coordination meeting at 10AM. Confirm location lock."
Coach: "Schedule updated for Saturday."

Upcoming Events
Game vs LA on Friday • Press shoot at 4PM • Contract signing Q&A on Zoom this weekend.

Activity Logs
Last login: Brooklyn, NY (3:47AM)
Device: MacOS • Session: Secure
Audit log synced.

Inner Circle Access
Agent, Lawyer, Manager: all access verified. Tap to revoke permissions or add authorized rep.

Legal + Insurance
Liability waivers, travel coverage, personal injury policies — all up to date as of June 1.

Still Having Issues?
For assistance with MFA setup, contact:
helpdesk@falconisecurity.com
(555) 123-4567
9 AM – 5 PM EST, Mon–Fri