Backup Strategy Plan

Version 1.0

Prepared by: Luigi Falconi,

Chief Information Security Officer

June 26th, 2025

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

Document Revision History

Date	Version	Description	Author
6/26/2025	1.0	Falconi Sports Agency Backup Strategy Plan	Luigi Falconi, CISO

FALCONI
SPORTS AGENCY

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

Table of Contents

FALCONI
SPORTS AGENCY

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

1. Objective

To ensure data confidentiality, integrity, and availability of Falconi's digital assets, we will implement a hybrid backup strategy that uses both local and cloud-based options. This ensures resilience in the face of cyberattacks, accidental deletion, or hardware failure, and a fast recovery of critical business systems while staying aligned with best practices and compliance requirements.

This policy applies to all employees, departments, and systems at Falconi Sports Agency. It covers data generated by daily operations, including internal staff information, client records, communications, and system logs.

2. Key Terms

Backup	A copy of data stored separately from the original system that can be used to restore information in the event of data loss caused by hardware failure, cyberattacks, or accidental deletion.
Backup Types:	• Full: All selected data is backed up • Differential: Only data modified since last full backup is saved • Incremental: Only data modified since the last backup (any type) is saved.
Network Attached Storage	A local storage device connected to the network allowing for centralized data backup and access

AES-256 Encryption	A method of securing our backups by turning data into unreadable code that can only be read using a secure key. It ensures the contents of our backups remain hidden in the event of unauthorized access.
TLS Encryption	A method of securing our data by making it unreadable while it is being transferred over the internet. This ensures our backups can't be read or intercepted while syncing to our cloud storage systems.
Recovery Time Objective	The maximum acceptable amount of time it should take to restore a system or data after a disruption
Recover Point Objective	The maximum acceptable amount of data that can be lost due a disruption without causing Falconi significant harm
NFLPA	The labor union representing NFL athletes is responsible for overseeing compliance with data protection standards for athlete information.

3. Data to Be Backed Up

This plan applies to all critical company data, including:

Data Category	Assets	Criticality	Frequency	Type

Employee	Employee Info	Moderate	Weekly	Full
	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
Business Operations	CRM	Critical	Daily	Full
	Athlete Analytics Software	High	Weekly	Incremental
	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

4. Data Retention Policy

Data Category	Assets	Retention Period
Employee	Employee Info	5 years
	Employee Payroll	7 years
	Employee Contracts	7 years
Client	Client Info	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)

5. Backup Strategy

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

6. Recovery Process

- **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 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.

7. Roles and Responsibilities

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.

8. Testing and Maintenance

To ensure the reliability and effectiveness of Falconi's backup systems, testing and maintenance will be as follows:

Monthly backup test:

- A restoration test will be performed on both local and cloud backups once a month.
- The goal is to verify the integrity of the backed-up data and ensure there are no errors or issues with the recovery process.
- Any errors or failed restorations will be documented and addressed immediately.

Biannually Backup Simulation:

- Full restorations will be conducted using offsite backups.
- This comprehensive disaster recovery simulation will test the recovery of critical systems and data under realistic failure scenarios.
- This test will confirm that all critical systems and data can be successfully restored in accordance with Falconi's RPO and RTO.

Change-driven reviews:

- Backup procedures and frequencies will be reviewed and updated immediately following any:
    - Major software upgrades
    - Hardware replacements
    - Introduction of new systems or platforms
- This ensures that all new or modified systems are incorporated into the backup strategy and protected in accordance with Falconi's established backup policy.

9. Additional Notes

- All backups are encrypted using AES-256 encryption and protected with access-controls to prevent unauthorized use and modification
- All backup files and snapshots will be timestamped with their creation date and labeled according to backup type (Full, Incremental, or Differential).
- Only the IT Admin and CISO have write permissions to backup files; all other employees have read-only access to backup files as needed
- Backup logs are reviewed weekly to verify success of scheduled backups and to identify any backup failures
- Automated alerts are in place in case of backup failure or missed scheduled backup

- Backup credentials are stored securely using an authorized password manager
- This backup policy is reviewed and approved by the Chief Information Security Officer

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

10. Acknowledgment

- I acknowledge that I have read and understood the Falconi Backup Strategy Plan and the procedures outlined for data backup, restoration, and retention.
- I understand that Falconi uses a hybrid backup approach including local NAS, cloud-based systems, and offsite storage, all encrypted using AES-256 encryption and monitored for compliance.
- I agree to follow all company-approved data storage and backup procedures, including the use of designated folders, avoiding the storage of company files on personal devices or unauthorized cloud services.
- I understand that monthly and biannual restoration tests are conducted to ensure the integrity of backups, and that I may be required to support recovery verification efforts in my role.
- I will report any backup errors, unauthorized access, or data integrity issues to the IT Admin or CISO immediately.
- I understand that only designated personnel (IT Admin and CISO) have write access to backup data, and all employees must comply with the access controls in place.
- I understand that failure to comply with this backup policy may result in disciplinary action, including possible termination and legal consequences.

❑ By acknowledging this policy, I agree to adhere to the responsibilities and security protocols outlined in this document.

Name Date

FALCONI
SPORTS AGENCY

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