Felcorp support

SECURITY GUIDE

Client data security for financial planning firms

What to set up before outsourcing, and how Felcorp protects your data at every step.

ISO 27001

together we grow

Certified information security management across all Felcorp operations.

Table of contents

PART 1: YOUR SECURITY SETUP

Before you outsource: the security foundation 3

- Identity and access management 3
- Endpoint and device security 3
- Data protection and storage 4
- Application access controls 4
- Pre-outsourcing readiness checklist 5

PART 2: FELCORP'S SECURITY FRAMEWORK

How Felcorp protects your data 6

- Technology and endpoint security 6
- People and process controls 7
- Monitoring, audit and incident response 8
- Contractual protections 8

THE REAL-WORLD BALANCE

Security, efficiency and risk 9

- Where over-restriction creates real problems 9
- Email: the single biggest vulnerability in outsourced operations 7

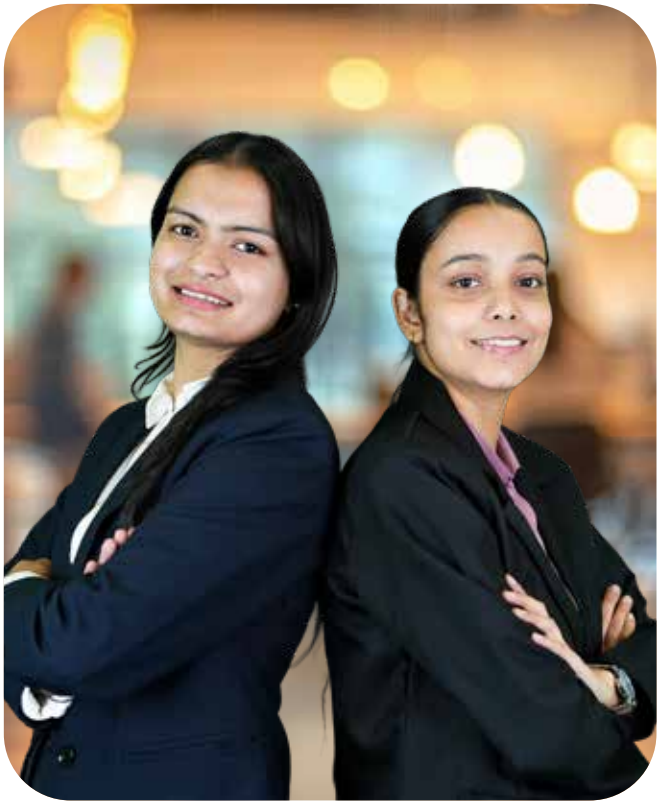
APPENDIX

Security setup and maturity checklist A-1

PART 1

Table of contents

What financial planning firms should have in place before outsourcing any client facing or back-office operations.



83%

of data breaches in financial services involve compromised credentials.

Source: IBM Cost of a Data Breach 2024

$5.9M

average cost of a data breach in the financial sector.

Source: IBM Cost of a Data Breach 2024

91%

Multi-factor authentication blocks over 99% of credential-based attacks.

Source: IBM Cost of a Data Breach 2024

Before you outsource: the security foundation

Outsourcing does not remove accountability, it extends your security. Strong internal controls ensure your BPO team operates safely from day one, not as a risk.

Identity and access management

Your identity layer is your first and most critical defense. If your BPO team relies on shared passwords without a second factor, every other security control is weakened.

- **Enforce multi-factor authentication (MFA):** On every account your outsourced team uses. SMS works, but authenticator apps or hardware keys provide
- **Use named accounts, not shared logins:** Everyone accessing your systems must have individual credentials, shared accounts eliminate accountability
- **Apply least-privilege access:** Your BPO team should only see the data and systems they need for their specific tasks. Start narrow and expand if needed.
- **Set up conditional access policies:** That restrict logins to approved devices, locations or IP ranges. This prevents credential use from unexpected

Data protection and storage

Financial planning data is highly sensitive. Client portfolios, tax file numbers, bank details and estate plans all contain critical personal information.

Before sharing it with a BPO provider, know exactly where your data is stored and who can access it.

Role-based access

Define roles in each application that match the tasks your BPO team performs. Do not give admin access by default.

Session timeouts

Set automatic lockouts after 15 minutes of inactivity. Idle sessions on shared floors are a real risk vector.

Audit logging

Enable detailed access logs in every system your BPO team uses. You should be able to see who accessed what and when.

Application access controls

Your practice management platform, CRM, document storage and email are the four systems most commonly accessed by outsourced teams. Each one needs its own access policy.

Why this matters for financial planning specifically

Financial planners hold a duty of care that extends beyond standard business data protection. Your clients trust you with the full picture of their financial lives. When you outsource, that trust transfers. The controls above ensure the transfer is secure and auditable.

Pre-outsourcing readiness checklist

Use this checklist to verify your security posture before onboarding any BPO provider. Each item should be confirmed, not assumed.

Security readiness checklist for financial planning firms

Identity & Access

- MFA enforced on all accounts the BPO team will use
- Named accounts created (no shared logins)
- Least-privilege access configured per role
- Conditional access policies active (device/location restrictions)

Endpoints & Devices

- EDR deployed on all BPO-accessible devices
- Full-disk encryption enabled
- Automatic updates enforced
- USB and local download restrictions applied

Data Protection

- Encryption at rest (AES-256) and in transit (TLS 1.2+)
- Data classification tiers defined
- Export/download restrictions in place
- Data processing register documented

PART 2

Felcorp’s security framework

How we protect your client data across technology, people, processes and contractual safeguards.

Technology

EDR, encryption, access controls, network security

People

Vetting, NDAs, training, secure on/offboarding

Process

SIEM monitoring, audits, incident response

Data Protection

Vetting, NDAs, training, secure on/offboarding

“Security in outsourcing is not about having the right tools. It is about having the right habits. We train for the habits, then verify them continuously.”

Tobias Fellas | Founder & CEO, Felcorp Support

How Felcorp protects your data

Security is not an add-on at Felcorp. It is built into the infrastructure, the hiring process, the daily operations and the contractual framework.

Every control below is active across all client engagements, not offered as an optional upgrade.

Technology and endpoint security

All Felcorp devices are company-owned and fully secured, with no personal access. Systems are monitored 24/7, encryption is enforced, data transfer is restricted, and updates are applied promptly.

Control	Implementation	Why it matters
Network segmentation	Client environments run on dedicated VLANs with firewall protected segmentation.	A breach in one engagement cannot spread to another client's data.
DNS filtering	All outbound traffic passes through Cisco Umbrella with category-based blocking.	Prevents access to malicious sites, phishing domains and unauthorised file sharing.
VPN access	Split-tunnel VPN with MFA required for every session. No persistent connections.	Ensures encrypted, authenticated access even from remote locations.
DLP policies	Microsoft Purview DLP monitors email, Teams, and file uploads for sensitive data.	Catches accidental or intentional data leakage before it leaves the network.

People and process controls

Technology only works when the people using it are trained, vetted and held accountable. Felcorp's people controls are designed to prevent insider risk while maintaining the operational speed your firm needs.

Pre-employment screening

All Felcorp team members undergo background checks, including identity, criminal, and reference verification before client assignment. Additional credit checks are conducted for financial services roles where permitted.

Confidentiality agreements

All staff sign binding NDAs that cover client data, proprietary processes and business information. These agreements survive termination of employment and are enforceable in the relevant jurisdiction.

Security awareness training

Mandatory training at onboarding and quarterly refreshers covering phishing recognition, social engineering, data handling procedures and incident reporting. Completion is tracked and non-completion triggers access suspension.

Secure onboarding and offboarding

Access is provisioned on the first day using pre-configured role templates. On departure or reassignment, access is revoked within 4 hours. Hardware is wiped and re-imaged before reissue.

Monitoring, audit and incident response

We monitor access patterns, data movements and system behaviour continuously. Security is not a periodic audit for us. It is a live operation.

24/7 SIEM monitoring

All security events are collected, correlated and analysed in real time. Anomalous behaviour triggers automated alerts and manual investigation.

Annual penetration testing

Third-party security firms test our infrastructure and application security. Results and remediation plans are available to clients on request.

- **Data processing agreements (DPAs)** that define scope, retention, deletion and sub-processor disclosure obligations.stronger security.
- **Service level agreements (SLAs)** with measurable security metrics including uptime, incident response times and access revocation windows.
- **Right to audit clauses** that allow your firm (or your auditor) to inspect Felcorp's security controls, processes and compliance documentation.
- **Breach notification commitments** with defined timelines (typically 24-72 hours) aligned to your regulatory obligations.

The real-world balance: security, efficiency and risk

Security controls always add some friction. The goal is to balance strong protection with minimal disruption. Too many restrictions slow work and reduce efficiency, while too little control increases risk and exposure.

Where over-restriction creates real problems

Over-restriction creates real problems. High-security policies protect data but also add friction, especially for high-volume outsourced teams. These are the most common inefficiencies we see.

- **Over-granular access controls** When every new task requires a fresh access request and 48-hour IT turnaround, your BPO team sits idle. Build role templates broad enough to cover the full scope of work, not individual actions.
- **Session timeouts that are too aggressive** A 5 minute timeout on a practice management system means your team re-authenticates 30+ times per day. 15 minutes is the standard balance point.
- **Approval chains for routine actions** If your outsourced team needs a manager's sign-off to send a standard client letter, you have built a bottleneck into every task. Pre-approve templates and reserve approvals for exceptions.
- **Blocked clipboard and copy-paste** DLP policies that prevent all copy-paste between applications make data entry painfully slow. Target the restriction to sensitive fields (account numbers, TFNs) rather than blanket-blocking everything.

Ready to outsource with confidence?

Talk to our team about your security requirements. We will walk you through our controls, answer your compliance questions and help you build an outsourcing arrangement that your clients, auditors and regulators can trust.

Start a security conversation

ALSO IN THIS SERIES

Security Guide for Accounting Firms

Security Guide for Insurance Firms

Compliance Guide: Australia (APRA CPS 234)

Compliance Guide: United States (SEC/FINRA)

Compliance Guide: United Kingdom (FCA)

How to use this checklist

Minimum for outsourcing: every control should be at "Managed" or above before your BPO team goes live. Items still at "Basic" represent active risk that should be remediated first.

Target state: work toward "Mature" across all controls over 6-12 months. Your Felcorp account manager can help prioritise the sequence based on your firm's specific risk profile and regulatory environment.

APPENDIX A

Security setup and maturity checklist

Use this checklist to assess your security posture and identify gaps before outsourcing. Rate each item across three maturity levels and focus on anything below “Managed” before go-live.

Control	Basic	Managed	Mature
Identity & Access Management			
Multi-factor authentication	MFA on email only.	MFA on all cloud apps. SMS based.	MFA enabled on all apps with conditional access in place.
Account management	Shared logins exist for some systems.	Named accounts for all users.Manual provisioning.	Named accounts, automated provisioning/deprovisioning, quarterly access reviews.
Privilege levels	Most users have admin or broad access.	Role-based access defined. Some over provisioning.	Least-privilege enforced. Just-in time access for elevated permissions.
Password policy	No enforced password requirements.	Minimum length and complexity enforced. Annual rotation.	Passphrase policy. Password manager mandated. No rotation (NIST aligned).

FELCORP SUPPORT

felcorp.com

hello@felcorpsupport.com

CERTIFIED
ISO 27001

CERTIFIED
SOC 2 Type II

“All risks can be satisfactorily mitigated. Asking the right questions, putting in the right procedures and having a clean, simple process is the key steps to reducing risk.”

Tobias Fellas | Founder & CEO, Felcorp Support