THE FINO PARTNERS

PHONE: +1-866-906-1314
WEB: www.thefinopartners.com
Email: hello@thefinopartners.com
ADDR: 16192, Coastal Highway, Lewes
Delaware 19958 U.S.A

Information Security Policy

1 Purpose

The purpose of this Information Security Policy is to define the framework used by The Fino Partners to protect information assets, including confidential client data belonging to US CPA firms, accounting firms, and other entities. This policy is intended to reduce the risk of unauthorized access, misuse, disclosure, alteration, or loss of information while supporting secure offshore service delivery through a ***resource-based engagement model.***

Under this model, personnel provided by The Fino Partners may be assigned on a dedicated or semi-dedicated basis to client teams and perform work under client instructions, while remaining subject to The Fino Partners' security, confidentiality, and compliance requirements.

2 Scope

This policy applies to all employees, contractors, offshore consultants, interns, temporary staff, and any other individuals engaged by The Fino Partners, including resources assigned to clients under a resource-based or staff-augmentation model.

It covers all information assets, systems, devices, applications, networks, cloud platforms, and communication tools used in the course of business, whether accessed through The Fino Partners' internal systems or client-provided systems, and whether work is performed from office locations or remote work environments.

3 Information Security Principles

The Fino Partners follows generally accepted information security principles to guide its controls and practices. Information is protected to ensure confidentiality, integrity, and availability throughout its lifecycle.

Security measures are designed to be reasonable, appropriate to risk, and aligned with contractual obligations and security expectations defined by clients, particularly where resources operate as part of client-directed teams.

4 Information Classification and Handling

Information handled by The Fino Partners is classified based on sensitivity and business impact. Client financial data, tax records, personally identifiable information (PII), credentials, and proprietary materials are treated as confidential and receive the highest level of protection.

Confidential information may be accessed only for legitimate business purposes and only by authorized resources assigned to the relevant client or engagement. Such information must not be shared, copied, or stored outside approved systems unless explicitly authorized by The Fino Partners and, where applicable, by the client. Internal and public information must also be handled responsibly to prevent misuse or unintended disclosure.

THE FINO PARTNERS

PHONE: +1-866-906-1314
WEB: www.thefinopartners.com
Email: hello@thefinopartners.com
ADDR: 16192, Coastal Highway, Lewes
Delaware 19958 U.S.A

5 Access Control and User Management

Access to information systems is granted based on job roles, client-approved responsibilities, and business requirements, following the principle of least privilege.

Resources assigned under the resource-based model are provided access only to the systems, data, and environments necessary to perform client-authorized duties. Unique user credentials are required for system access, and sharing of login information is prohibited.

Access rights are reviewed periodically and are promptly revoked when an individual's employment or engagement ends, when a resource is reassigned, or when access is no longer required by the client or The Fino Partners.

6 Authentication and Password Practices

Users are required to follow established authentication and password practices to protect system access. Passwords must be kept confidential and must not be shared, written down, or stored insecurely.

Additional security controls, such as multi-factor authentication and encryption, are implemented based on system sensitivity, client requirements, and the nature of access granted to assigned resources.

7 Device and Endpoint Security

Company-approved devices must be used to access company and client systems unless client-approved exceptions apply. Reasonable security controls, including password protection, antivirus software, and system updates, must be maintained on all devices used for work.

Resources must not disable or bypass security controls. Any loss, theft, or suspected compromise of a device used for client or company work must be reported promptly so that appropriate protective action can be taken.

8 Network and System Security

Access to company and client systems must occur through secure and approved connections. Reasonable technical safeguards, such as encryption, firewalls, and monitoring, are implemented to protect systems from unauthorized access and cyber threats.

Use of unsecured public networks to access sensitive client or company information should be avoided. System activity may be logged and reviewed for security, compliance, and client assurance purposes.

8 Remote Work and Offshore Security Controls

For remote and offshore operations, resources are responsible for maintaining a secure working environment consistent with both internal security standards and client expectations.

Client information must not be accessed or discussed in public places, and screens must not be visible to unauthorized individuals. Printing or physical storage of client data outside approved office locations is not permitted unless explicitly authorized. Remote work practices must align with client confidentiality requirements applicable to assigned resources.

THE FINO PARTNERS

PHONE: +1-866-906-1314
WEB: www.thefinopartners.com
Email: hello@thefinopartners.com
ADDR: 16192, Coastal Highway, Lewes
Delaware 19958 U.S.A

10 Data Storage, Retention, and Disposal

Information is stored only on approved systems and platforms, including client-provided environments where applicable. Data is retained only for as long as required to meet business, contractual, or legal obligations.

When information is no longer required, it is disposed of using reasonable and secure methods to prevent unauthorized recovery. Physical records, if any, must be destroyed in a secure manner.

11 Email, Communication, and Data Transfer

Business communications involving client or confidential information must occur only through approved communication channels designated by The Fino Partners or the client.

Personal email accounts, messaging applications, or unapproved file-sharing tools must not be used for transmitting business or client data. Resources must take reasonable care to ensure information is shared only with authorized recipients and that sensitive data is protected during transmission.

12 Third-Party and Client System Access

Access to client systems is governed by contractual agreements and documented client instructions. Resources assigned to clients must comply with all client-specific security, access, and acceptable-use requirements.

Client credentials must be kept confidential and used only for authorized purposes. Any security concern related to client systems must be reported promptly to The Fino Partners.

13 Security Incident Management

Any actual or suspected security incident, including data breaches, unauthorized access, malware infections, or data loss, must be reported immediately to management.

The Fino Partners will take appropriate steps to investigate incidents, coordinate with affected clients where required, mitigate impact, and implement corrective measures to reduce future risk.

14 Training and Awareness

Employees and assigned resources are expected to complete periodic information security training relevant to their roles and client assignments.

Ongoing awareness efforts are used to promote secure handling of information and to reinforce individual responsibility for protecting client and company data.

THE FINO PARTNERS

PHONE: +1-866-906-1314
WEB: www.thefinopartners.com
Email: hello@thefinopartners.com
ADDR: 16192, Coastal Highway, Lewes
Delaware 19958 U.S.A

15 Legal, Regulatory, and Contractual Compliance

The Fino Partners is committed to complying with applicable laws related to data protection and cybersecurity. The firm also aligns its security practices with contractual confidentiality and information security obligations agreed upon with US CPA firms, accounting firms, and other clients.

This policy supports client compliance requirements without transferring regulatory responsibility beyond contractual scope.

16 Monitoring and Audit

Information systems and access may be monitored to ensure compliance with this policy, protect client information, and maintain operational security, subject to applicable laws.

Periodic internal reviews may be conducted to identify security risks, including those arising from client-assigned access under the resource-based model.

17 Policy Violations and Disciplinary Action

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract. Serious violations may also lead to legal or contractual consequences, including client escalation.

18 Policy Review and Updates

This policy is reviewed periodically and updated as necessary to reflect changes in business operations, service delivery models, technology, legal requirements, or client expectations.

For Fino Partners Group, Inc.

CEO, Founder

For Fino Partners Group, Inc.

COO, Founder