Information Security Policy

Document Owner: Jack Ryan

Effective Date: June 1, 2020

Version: 2.1

Document Approver: Carolyn Nohe

Table of Contents

Introduction

FinGoal Serves Trusted Financial Brands

FinGoal analyzes account holder credit and debit card spending in order to best understand each user at an individual level and match them with automated insights, advice, and recommendations to optimize their daily spending. Additionally, FinGoal can use this understanding of the user to help their financial institution better serve the user.

Upon consumer authorization, FinGoal is sent feeds of consumer transactions from checking and credit accounts. At no point does FinGoal ever transmit or hold a customer's account numbers or password. FinGoal does not hold money for customers.

Although FinGoal never touches a user's most financial sensitive information (e.g. SSN or card numbers), we do hold something equally important: their trust. As a white-labeled solution serving trusted financial brands, FinGoal must act with great care and stewardship over the entire data and experience flow.

In the interest of transparency, FinGoal makes our policies, controls, and architecture public. Security by obscurity has no place in modern financial services.

Access Control Policy

Access controls establish standards and procedures for preventing unauthorized access to information assets.

Access rights to FinGoal system components are limited to authorized personnel and are based on a user's role and responsibilities. Access rights to FinGoal system components must adhere to the concept of least privilege at all times. (For data classifications, see Types of Data.)

Least Privilege

The principle of least privilege grants users the bare minimum level of access to operating systems that is needed to perform their role or carry out their job responsibilities. FinGoal applies least privilege to its systems to add an additional layer of security over the data and information that a user handles and to reduce the risk of users abusing their access privileges.

Privileged Users

Privileged users are those with elevated or superuser access to in-scope systems and system components that is granted according to business needs. Privileged users (e.g., system administrators, IT engineers) are responsible for ensuring that the access rights for all users are commensurate with the following:

- The user's role and responsibilities within FinGoal (this principle is known as role-based access control)
- The concept of least privilege and separation of rights based on job duties

Provisioning Users

When an employee or contractor joins FinGoal, they are given the appropriate tools and access to FinGoal systems. During the process of onboarding, employees are assigned unique identifications (ID) and are sent the organization's policies. Employees must acknowledge having read and received the policies before being granted access to the information systems and networks needed to carry out their roles and responsibilities.

Users for all in-scope systems and system components are provisioned using all applicable provisioning and de-provisioning tools as necessary.

In-scope systems include the following:

- Organizational networks
- Applications
- Operating systems (OS)
- Data stores
- Cloud service provider (CSP) console
- Encryption keys
- Firewalls
- Log data

User Identifications

When a new user is onboarded, they are assigned a unique FinGoal employee ID. This ID defaults to the user's first name in lowercase text. If that ID already exists, then the ID will be the user's first and last name.

Employees are strictly prohibited from sharing IDs or from using another user's ID, regardless of whether the other user has granted permission.

User Access

Once an ID has been assigned to a new user, a formal access request ticket or email must be submitted to and approved by the appropriate system owner or a manager. When the access request is approved, the new user is given access to their FinGoal email, internal resources, and any other elevated permissions that their role requires them to have.

This same process is applied when existing employees require additional levels of access.

Deprovisioning Users

For any modifications to or removal of access, a formal access request ticket or email is required to ensure these actions are documented and completed in a timely manner. Terminated employees have access revoked within twenty-four (24) hours of termination.

Access Review Policy

All employee access to production systems is reviewed by management at least semi-annually to confirm the access of each employee is appropriate and complies with the principles of least privilege and separation of duties.

The access review and any modifications to system access are formally documented and tracked.

Identification and Authentication Policy

All users are authenticated through unique IDs and passwords or through authorized secure shell (SSH) keys in order to access FinGoal's information systems and networks.

FinGoal uses automated access control systems to restrict user access to its network and data. These automated access controls require users to authenticate before they may access any of the following:

- FinGoal's network
- FinGoal's source code
- FinGoal's and its customer data
- Other restricted data

All users must use multi-factor authentication (MFA) measures to ensure that access to in-scope system components are protected at all times. MFA is met by incorporating two (2) of the three (3) methods of authentication listed below:

- **Something a user knows:** Generally includes passwords, passphrases, personal identification numbers (PIN), or some other type of knowledge that is known by a user
- **Something a user has:** Generally includes some physical attribute provided to a user (e.g., access card, badge reader, key fob, dynamically generated unique identifier)
- **Something a user is:** Generally includes a unique physical attribute of the user, commonly known as biometrics. Devices that read a user's biometrics for authentication include, but are not limited to, the following:
    - Iris scanners
    - Palm scanners

    - Fingerprint readers
    - Facial recognition utilities
    - Voice recognition devices

The use of non-authenticated user IDs (i.e., IDs with no password or security token) or user IDs not associated with a single identified user is prohibited. Shared or group user IDs are never permitted for user-level access unless approved by authorized personnel.

Password Policy

Passwords are a critical component of information security. Passwords protect user accounts and must be configured according to FinGoal's password policies. FinGoal requires users to create and use complex passwords.

Passwords must be safeguarded, and owners should not share them with other users. Passwords used by all users must meet or exceed all stated FinGoal policies for password complexity requirements.

Password Complexity

FinGoal requires that all passwords meet or exceed all of the following guidelines:

- Contain at least eight (8) alphanumeric characters, one of which must be a number
- Contain both upper and lowercase letters
- Contain at least one special character (e.g., $%^&*()_+|~-=\`{}[]:";'<>?,/).

A poorly constructed password is weak and may result in the compromise of systems and data; weak passwords are therefore prohibited. Weak passwords have the following characteristics:

- Contain fewer than eight characters
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, etc.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software

Invalid Password Lockouts

Parameters regarding account lockout policies and password resets are enforced with system settings. Only authorized personnel are allowed to make any changes to the password complexity rules and lockout policies.

Remote Access to Production Systems

All access to FinGoal system components initiated outside the organization's trusted network infrastructure is considered "remote access.” Remote access to production systems is restricted to authorized employees with a valid MFA token.

All users must use approved technologies, such as internet protocol security (IPSec) and/or secure socket layer (SSL) virtual private networks (VPN) for remote access. These approved protocols are to be used along with MFA and additional supporting measures such as secure shell keys (SSH).

Change Management Policy

Configuration Management

FinGoal defines “configuration management” as the establishment, implementation, maintenance, recording, and monitoring of secure configurations in the organization’s information landscape. This landscape includes, but is not limited to, all network devices, operating systems, applications, and internally developed software and systems (e.g., firewalls, servers, databases). If any specific systems are complex or large enough to require their own configuration management program, they are developed independently by authorized personnel and abide by the practices stated in this policy.

System Hardening

FinGoal adopts its system hardening settings from the most restrictive baselines from Center for Internet Security (CIS), National Institute of Standards and Technology (NIST), and/or public CSP baseline configurations.

Authorized Engineering personnel support the configuration management program by identifying the following:

- The minimum security settings for ensuring a risk level as low as possible that still allows the organization to operate in an efficient and effective manner
- Baseline configuration standards for system resources in consultation with vendor-specific guides and respected industry benchmarks, frameworks, and associations
- Insecure services, ports, and protocols for all in-scope system components. This identification requires a strong technical understanding of all relevant operating systems, network devices (e.g., firewalls, routers, switches, load balancers), and applications (e.g., web server applications, database applications)

Changes to configuration settings are monitored and controlled according to FinGoal's System Change Management Policy and procedures. Automatic deployment mechanisms harden systems to assure consistent application of configuration standards from the moment of deployment.

Secure System Development Life Cycle Policy

This policy describes at a high level how FinGoal approaches product development. Any members of the product team (e.g., Product Manager) are referred to as "Product"; any members of the engineering team (e.g., Engineer Manager, Developer) are referred to as "Engineering."

Network Segregation

The development, staging, and production environments are appropriately segregated. Development uses multiple separate environments to stage changes before being pushed into production to ensure that untested code is not released in the primary system. Multiple safeguards exist to ensure that data and code are not compromised at each stage of the development pipeline. Sensitive and Confidential data is prohibited from use in the development and/or test environment.

System Change Management Policy

Identification and Prioritization

The primary reasons for product change requests include, but are not limited to, the following:

- Strategic product development roadmap, defined by FinGoal's senior management team
- Input from users
- Internally driven innovation activities that result in new or updated features
- Input from employees and relevant stakeholders (e.g., advisors)
- Routine maintenance

Product is responsible for collecting change requests. During regular product management meetings, Product reviews requested changes, groups related changes into features, captures any versioning, and assesses operational impacts and dependencies. They may consult executive leadership, Engineering, and/or other FinGoal stakeholders to evaluate further the risks and technical impacts of changes. These discussions inform the prioritization schedule for upcoming development efforts.

Product and Engineering maintain product change requests in a centralized, secure system of record. For each change request, Product details specifications and assigns classifications and ownership to each item in supporting documentation. At a minimum, for each change request, Product ensures that the following information is recorded:

- A feature title and description
- Classification (e.g., emergency, critical, major, minor)
- Governance, including Product, Engineering, and any other applicable cross-functional stakeholders
- Risk, impacts, and dependencies associated with the feature
- Links to systems and documents related to the feature (e.g., requirements, GitHub Issues)

Specification and Review

Product is responsible for defining and documenting requirements for each product change request associated with their assigned application. Once Product completes the initial draft, they send the request to Engineering for refinement and assignment. Engineering assesses the change request for feasibility and works with Product to strengthen the approach and to further detail any needed changes.

The CTO has final approval over requirements for all changes classified as emergency, critical, or major.

Development Cycles

Engineering develops a change during a development cycle (e.g., a sprint). During the cycle, Engineering manages items from the start of development through completion. Although FinGoal promotes pre-planning, its Engineers also have the ability to modify their approaches in real time, so long as such modifications continue to meet requirements and quality standards. While developing the changes, Engineers write tests for simulated scenarios that automatically check the expected results against targeted requirements during and following the development cycles.

Continuous Deployment

FinGoal uses a continuous deployment approach. A single change request by Product is typically deconstructed by Engineering into a collection of individual implementation and configuration changes (e.g., tasks), each of which is individually tracked and deployed to production through a unique change request record (e.g., a GitHub Pull Request). All changes in implementation or configuration are subject to the continuous deployment process.

Pre-Implementation Testing

Engineering continuously deploys changes that are ready for testing in the staging environment. Depending on the nature of an issue identified in testing, Engineering has the authority to make fixes in real time.

Validation efforts in this environment consist of automated functionality and security testing.

Approval

FinGoal seeks to produce new releases swiftly yet with the oversight necessary to promote quality and assure adequate controls:

- Before pushing a release to production, the CTO must approve changes classified as having a major impact.
- Any visible changes to end-user-facing documents and interfaces are automatically cataloged and require manual review and approval.
- All changes in implementation or configuration require approval by a second member of Engineering who did not implement the change.
- A successful execution, completed during the pre-implementation testing phase, is required for releasing a feature in production.

Staging Deployment

After obtaining final approval, the change is deployed to a staging environment whose configuration fully mimics the production environment. Multiple changes may be bundled automatically into a single deployment to facilitate rapid development and iteration.

Validation is achieved in this environment by a successful deployment of all requested changes, followed by automated testing that simulates user behavior. Successful completion of all staging tests initiates deployment to the production environment.

Production Deployment and Communication

Once a staging deployment has been successful, an identical deployment is initiated in the production environment.

- If the deployment succeeds with no errors, the change request is marked as successfully merged, the Git version control system is updated to reflect the changes, and Engineering is notified of the change.
- If the deployment encounters an error, any changes are automatically rolled back and the implementer is notified of the failure. Once a defect has been repaired or a feature has been fully realized by Engineering, Product members associated with the change request are notified that the change is complete, and the system of record is updated.

Rollback Procedures

FinGoal's ability to execute rollback procedures depends on the change(s) that need to be rolled back. If a rollback is possible, Engineering is able to address an issue in near real time by reverting to a previous version of the product.

Continuous Improvement

Although the System Change Management Policy presents the change management process linearly, FinGoal accumulates feedback throughout the system development process, reviews and prioritizes requested changes, and reflects those changes as incremental improvements to the product. Moreover, FinGoal runs feature development simultaneously, with Product and Engineering focusing on their respective portions of the platform.

Inventory Management Policy

FinGoal's management maintains a system asset inventory that does the following:

- Accurately reflects the organization’s production systems
- Includes all system components
- Does not duplicate components that appear in multiple systems
- Maintains enough information to track and report on assets – in particular, marking relevant assets as “critical” and verifying that they meet security baseline requirements
- Indicates whether assets store or access Sensitive and/or Confidential data (as defined in the Network and System Security Policy)
- Notes any approved deviations to current deployed configurations
- Assigns ownership of system components and documents assignees’ acknowledgment of ownership
- Documents accountability information, including responsibility and ownership, by name, position, or role

Change Communication

FinGoal communicates any major changes to the system to authorized internal users (e.g., feature releases).

For major system changes, FinGoal follows these steps:

- Obtains final approvals from authorized staff
- Deploys the feature in either the organization’s internal production environment or in a customer’s environment (in conjunction with the customer’s personnel)
- Sends release notes that describe the functionality introduced with the release, provide examples of how to use the new functionality, note fixes to material bugs identified during prior releases, and list known limitations

Corrective Action Policy

The FinGoal leadership team may develop and, in consultation with Human Resources, impose a corrective action plan upon noncompliant staff or other persons subject to the FinGoal Compliance Program as a means of facilitating the overall goal of full compliance.

Corrective Action Plans should be designed to first assist the noncompliant individual(s) to understand specific issues and reduce the likelihood of future noncompliance. Corrective action, however, shall be developed to effectively address the particular instance or issue of noncompliance and should reflect the severity of the noncompliance.

Elements of a Corrective Action Plan

The following constitute the minimum action which shall be taken in response to noncompliance with the Compliance plan. A Corrective Action Plan for a first violation of noncompliance shall include these elements:

- □ A clear statement of the specific problem(s) to be corrected.
- □ A summary of the method used that discovered the problem.
- □ A summary of the findings that include a root cause analysis of the noncompliance that will determine the extent and content of the Corrective Action Plan. The root cause may be found to include system or human error, negligence, reckless disregard of FinGoal policies or procedures, and applicable laws and regulations, or willful misconduct.
- □ Remediation, which at minimum, shall include additional education or training by the leadership team if a root cause analysis indicates that education or training is appropriate.
- □ Within ninety days after the remedial education is completed, a follow-up audit of the corrective action implementation to determine whether the Corrective Action Plan is being followed and is effective.
- □ A statement that the failure of an individual who is subject to a Corrective Action Plan to adhere to the plan shall be grounds for further corrective action that many include disciplinary procedures and/or actions.
- □ A statement that if a root cause analysis shows that the source of the problem was a reckless disregard for FinGoal or facility policies or willful misconduct, the Corrective Action policy shall yield to all appropriate provisions of the applicable Human Resources corrective action plans or policies.
- □ Documentation regarding Corrective Action Plans will be maintained by the leadership team for a minimum of 6 months after the completion of the plan.

Ethics & Anti-Corruption Policy

Whoever we may deal with, and wherever we may operate, we are committed to doing so lawfully, ethically and with integrity. As part of this commitment, all forms of bribery and corruption are unacceptable and will not be tolerated. We must not, and we must ensure that any third party acting on our behalf does not, act corruptly in our dealings with any other person. This anti-bribery and corruption policy sets out FinGoal’s policies to prevent acts of bribery and corruption. These policies and procedures have been designed to comply with legislation governing bribery and corruption on a global basis.

This policy provides guidance on the standards of behavior to which we must all adhere and most of these reflect the common sense and good business practices that we all work to in any event. This policy is designed to help you to identify when something is prohibited so that bribery and corruption is avoided, and provide you with help and guidance if you are unsure about whether there is a problem and you need further advice.

Scope

The fundamental standards of integrity under which we operate do not vary depending on where we work or who we are dealing with. This policy applies to all FinGoal officers, employees (full and part time) and temporary workers (such as consultants or contractors) (together referred to as “employees” in this document) across the group no matter where they are located or what they do. It is the responsibility of each of us to ensure that we comply with these standards in our daily working lives. This policy sets out a single standard that all employees must comply with, regardless of whether local law or practices might permit something to the contrary.

Part of FinGoal’s commitment to prevent bribery and corruption is to ensure that the people acting on our behalf also do so in compliance with effective anti-bribery and corruption policies. Accordingly, where we engage third parties such as agents, distributors or joint venture partners, we have obligations to complete sufficient due diligence when entering into arrangements to ensure that they are not acting corruptly, and to periodically monitor their performance to ensure ongoing compliance. In short, if we can’t do it, neither can they.

Failure to comply with this policy, whether or not this is intentional, may lead to disciplinary action (up to and including dismissal), and criminal liability for the individual involved (up to and including imprisonment). Employees will be required to confirm that they have read and understood the policy and that they comply with its terms as part of their ongoing employment assessment processes. In addition, relevant employees will be required to attend training to support the guidance in this policy.

Getting help

If you are unsure about your obligations under this policy, you should contact one of the following people for help:

- in the first instance, your manager; or

- legal@fingoal.com

Policy

What is bribery?

Bribery involves the following:

- when a financial or other advantage is offered, given or promised to another person with the intention to induce or reward them or another person to perform their responsibilities or duties improperly (it does not have to be the person to whom the bribe is offered that acts improperly); or
- when a financial or other advantage is requested, agreed to be received or accepted by another person with the intention of inducing or rewarding them or another person to perform their responsibilities or duties inappropriately (it does not have to be the person who receives the bribe that acts improperly).

It does not matter whether the bribe is:

- given or received directly or through a third party (such as someone acting on FinGoal’s behalf, for example an agent, distributor, supplier, joint venture partner or other intermediary); or
- for the benefit of the recipient or some other person.

Bribes can take many forms, for example:

- money (or cash equivalent such as shares);
- unreasonable gifts, entertainment or hospitality;
- kickbacks;
- unwarranted rebates or excessive commissions (e.g. to sales agents or marketing agents);
- unwarranted allowances or expenses;
- “facilitation” payments/payments made to perform their normal job more quickly and/or prioritize a particular customer;
- political/charitable contributions;
- uncompensated use of company services or facilities; or
- anything else of value.

This policy applies to both the public and private sectors. Dealing with public officials poses a particular high risk in relation to bribery and corruption and specific guidance when dealing with public officials is set out below. A breach of bribery laws can result in fines for both the company and the individual involved and in some jurisdictions could also result in imprisonment.

How do I know if something is a bribe?

In most circumstances, common sense will determine when a bribe is being offered. However, here are some questions you should ask yourself if in doubt:

- □ am I being asked to pay something or provide any other benefit over and above the cost of the services being performed, for an example an excessive commission, a lavish gift, a kickback or make a contribution to a charity or political organization?
- □ am I being asked to make a payment for services to someone other than the service provider?
- □ are the hospitality or gifts I am giving or receiving reasonable and justified? Would I be embarrassed to disclose them?
- □ when a payment or other benefit is being offered or received, do I know or suspect it is to induce or reward favorable treatment, to undermine an impartial decision making process or to persuade someone to do something that would not be in the proper performance of their job?

General prohibition

All forms of bribery and corruption are prohibited. We will not tolerate any act of bribery or corruption. Any breach of this policy or local law could result in disciplinary action being taken and ultimately could result in dismissal. A bribe does not actually have to take place - just promising to give a bribe or agreeing to receive one is prohibited.

Bribery is prohibited when dealing with any person whether they are in the public or private sector and the provisions of this policy are of general application. However, many countries have specific controls regarding dealing with public officials and this policy includes specific requirements in these circumstances.

Gifts, hospitality and expenses

Giving or receiving gifts or hospitality is often an important part of maintaining and developing business relationships. However, all gifts and hospitality should be for a genuine purpose, reasonable, given in the ordinary course of business and should comply with the FinGoal Hospitality and Expenses Policy and local laws.

Lavish or unreasonable gifts or hospitality, whether these are given or received, are unacceptable as they can create the impression that we are trying to obtain or receive favorable business treatment by providing individuals with personal benefits. In addition, gifts and hospitality can themselves be a bribe. Be careful to avoid even the appearance that the giving or accepting of gifts or hospitality might influence the decisions you take on behalf of FinGoal.

Facilitation payments

Facilitation payments are any payments, no matter how small, given to an official to increase the speed at which they do their job. For example, this could include speeding up customs clearance.

All facilitation payments are generally prohibited. However, your safety is our primary concern and we understand that there may be circumstances in which you have no alternative but to make a facilitation payment in order to protect against loss of life, limb or liberty. Any request for a facilitation payment should be reported to your manager.

Agent, distributors, suppliers and joint venture partners FinGoal could be liable for the acts of people that act on our behalf. This includes agents, distributors, suppliers and joint venture partners (together referred to as “third parties”). As such we are committed to promoting compliance with effective anti-bribery and corruption policies by all third parties acting on behalf of FinGoal.

All arrangements with third parties should be subject to clear contractual terms including specific provisions requiring them to comply with minimum standards and procedures in relation to bribery and corruption. Appropriate wording to be included in contracts can be obtained from Legal. You must not engage any third party who you know or reasonably suspect of engaging in bribery.

Appropriate due diligence should be undertaken before any third parties are engaged. The appropriate level of due diligence will vary depending on the circumstances and you should use your judgement on a case by case basis.

Questions you should be asking yourself include:

- □ who are they – have I seen documents evidencing that they are who they say they are?
- □ who else have they worked with – do they have references?
- □ are they well established with a good reputation or are they more obscure so that I need to do more to find out about them?
- □ do they operate in a territory where bribery is prevalent?
- □ are they happy to sign a contract agreeing to comply with anti bribery procedures? Do they have their own anti-bribery program?

- have I done basic searches such Google searches, business directory searches, etc?
- are there inconsistencies between the provider of the services and the person I am paying?
- are commissions/payments in line with generally accepted market practice?

Some high risk transactions will require further due diligence which may require independent investigation. Employees will be provided with helpful guidance and checklists where appropriate to support the due diligence process.

Entering into any joint venture arrangement without prior approval from FinGoal Legal is prohibited. All payments and commissions to third parties must:

- be made in accordance with the Group Authority Framework and the local policies relevant in your business as set by your line manager;
- be made via bank transfer through the accounts payable system and be fully accounted for;
- must be in line with generally accepted rates and business practice for the service in question and should not be unjustifiably excessive or unsupportable; and
- must be made in accordance with the terms of the contract with the person or company providing the services.

If you have any concerns that arrangements with a third party are not in accordance with this policy, you should ask your local anti-bribery and corruption officer for help.

Dealing with public officials

Although this policy applies to both public and private sectors, dealing with public officials poses a particularly high risk in relation to bribery due to the strict rules and regulations in many countries. Public officials include those in government departments, but also employees of government owned or controlled commercial enterprises, international organizations, political parties and political candidates. The provision of money or anything else of value, no matter how small, to any public official for the purpose of influencing them in their official capacity is prohibited.

The prior approval of FinGoal Legal is required in relation to:

- any payment in respect of fees, salary or commission (this does not include official fees);
- gifts and hospitality; and
- making charitable contributions in connection with dealings with a public official.

In addition, many public officials have their own rules regarding the acceptance of gifts and hospitality, etc, and we must respect these rules where applicable. In accordance with the FinGoal Code of Ethics, political donations by, or on behalf of, FinGoal are prohibited.

Compliance with the policy

It is the responsibility of your local anti-bribery and corruption officer to ensure compliance with this policy in each business. Ultimate responsibility for compliance with this policy throughout the group is taken by the Head of Legal. However, each of us has an obligation to act with integrity and to ensure that we understand and comply with the policy. Ongoing compliance will be monitored and reported by Internal Audit.

Training will be provided to relevant employees throughout the group to support them in complying with their responsibilities. If you are not selected for training but believe that it is relevant for you then please ask your local HR manager for further information. In addition, all employees will be required to confirm that they have understood and complied with the policy annually.

Whistleblowing

FinGoal is committed to ensuring that employees can speak up with confidence if they have any concerns or need to ask for help. If you suspect or observe anything that you think might be in contravention of this policy, you have an obligation to report it. You should raise your concerns with your local anti-bribery and corruption officer in the first instance. Alternatively, you can report your concerns under the Whistleblowing Policy.

FinGoal will not tolerate retaliation in any form against anyone for raising concerns or reporting what they genuinely believe to be improper, unethical or inappropriate behavior. All reports will be treated confidentially.

Government Data Request Policy

This policy is designed to inform and assist the FinGoal leadership team in the event that a government agency requests sensitive user information.

The way FinGoal responds to a request is contingent upon the situation. The leadership team should carefully review the request to make sure it satisfies applicable laws. If a request asks for too much information, it should be narrowed or, in some cases, rejected.

Scope

Only FinGoal leadership team members should be involved in this process. In the event that a member of the team is contacted by a government agency or official and asked to release sensitive information, they should under no circumstances share the data without first notifying and consulting with the leadership team including, but not limited to, the CISO and the CEO.

Policy

Upon receiving a request from a government agency, the leadership team must send an email to the user before disclosing information. If the account is managed by an organization, the leadership team must give notice to an account administrator.

However, FinGoal won’t give notice when legally prohibited under the terms of the request. The leadership team must provide notice after a legal prohibition is lifted, such as when a statutory or court-ordered gag period has expired.

FinGoal might not have to give notice if the account has been disabled or hijacked. Additionally, FinGoal might not give notice in the case of emergencies, such as threats to a child’s safety or threats to someone’s life, in which case the leadership team may provide notice if they learn that the emergency has passed.

If FinGoal's leadership team reasonably believe that they can prevent someone from dying or from suffering serious physical harm, they may provide information to a government agency — for example, in the case of bomb threats, school shootings, kidnappings, suicide prevention, and missing persons cases.

Incident Management Policy

FinGoal distinguishes between security events and security incidents as follows:

- **Security event:** A suspicious activity that deviates from normal behavior but does not appear to compromise any system resources. Security events include phishing emails, changes in login permissions, spikes in incoming traffic, and similar situations. Events may be elevated to incidents if determined by authorized personnel.
- **Security incident:** A suspicious or malicious activity that compromises a system resource and is being used for unauthorized purposes. Security incidents include data breaches, a successful distributed denial-of-service (DDOS) attack, or similar situations where the incident is so large that it may involve a legal team, public disclosure, or a failure to meet contractual commitments with customers.

Incident Management Roles and Responsibilities

The Incident Response Team (IRT) has clear roles and responsibilities for adequately preparing for and responding to any incident. The IRT follows the necessary steps, processes, and procedures to address an incident as well as to understand what actions (if any) to take with law enforcement agencies, local/federal/state agencies, the media, and any other third parties considered to be within scope.

The IRT is responsible for the following:

- Declaring a security incident
- Leading the incident response process after the incident is declared through a postmortem
- Determining what other teams or individuals are required to contribute to the response process
- Coordinating investigation and remediation efforts
- Keeping stakeholders informed

- Performing an annual test of the Incident Response program through a tabletop exercise

FinGoal’s IRT is to consist of the following assigned roles and respective responsibilities for effectively preparing for, detecting, responding to, containing, and recovering from an incident, including undertaking post-incident activities and awareness:

- **CTO:** Responsibilities include providing overall direction, leadership, and support for the organization’s entire incident response platform while also assisting other applicable personnel in their day-to-day operations. The CTO reports to other members of senior management on a regular basis on all aspects of the organization’s information systems posture, which includes incident response.
- **IRT Engineers and Systems Administrators:** Responsibilities are vitally critical for ensuring the safety and security of all enterprise-wide system resources in the event of a security incident. Responsibilities include implementing many of the operational, technical, and security procedures and related practices for incident response, such as:
    - Receiving incident alerts and making preparations immediately for responding to threats
    - Responding to threats by undertaking all necessary measures for ensuring the confidentiality, integrity, and availability of FinGoal’s critical system resources. This generally includes provisions for isolating and quarantining affected or suspected systems.
    - Assessing the severity of incidents and making necessary technical changes to critical system resources immediately for protecting other FinGoal assets

Incident Response Procedures

These procedures outline the steps necessary to address security and performance related events and incidents in order to ensure the confidentiality, integrity, and availability of FinGoal’s platform and supporting systems.

The IRT should follow the appropriate procedure based on the incident severity ranking:

- **Low:** Indicates attempted suspicious activity that did not compromise the network (e.g., a port scan or a failed intrusion attempt). Low severity is treated as a *security event*.
- **Medium:** Indicates suspicious activity that deviates from normally observed behavior and, depending on the use case, may be indicative of a resource compromise. Medium severity is treated initially as a *security event* but may be elevated to a *security incident*.

- **High:** Indicates the resource in question (e.g., an EC2 instance or a set of IAM user credentials) is compromised and is being used for unauthorized purposes. High severity is a true *security incident*.

Medium and Low Event Procedure

- □ **Initial response:** IRT reports incident to all internal staff
- □ **Investigation:** Investigates the issue
- □ **Internal notification:** Notifies all staff via phone, SMS, and Slack

High Security Incident Procedure

- □ **Initial response:** IRT reports incident to all internal staff
- □ **Documentation:** Raises a ticket in ticketing system and update as needed
- □ **Investigation:** Investigates the issue
- □ **Internal notification:** Notifies all staff via phone, SMS, and Slack
- □ **External notification:** Determines if notification to customers and authorities is necessary and, if so, sends notification

Business Continuity and Disaster Recovery (BC/DR) Plan Testing

FinGoal tests its business continuity (BC) capabilities on at least an annual basis.

The Business Continuity and Disaster Recovery Team is responsible for overseeing the execution and documentation of the annual BC/DR Plan test. FinGoal employs a tabletop exercise to simulate an unexpected service disruption to the product platform. Testing assesses the adequacy of FinGoal's BC/DR plans and associated procedures to do the following:

- Restore product accessibility
- Communicate with internal and external parties
- Recover data
- Support capacity needs for information processing, telecommunications, and environmental support in specified contingency conditions

FinGoal documents the results of the annual BC/DR Plan test through a post-simulation report that details the following:

- A description of the simulated service disruption

- A summary of FinGoal’s BC response actions
- Any identified issues and findings resulting from the BC/DR Plan test, including suggested updates
- FinGoal's performance against KPIs

Backup

FinGoal performs backups of Sensitive, Confidential, and Public data for all in-scope production systems, including infrastructure and data stores necessary to maintain service level agreements (SLA) with customers.

FinGoal configures its cloud service providers (CSP) Amazon Web Services (AWS), Google Cloud Platform (GCP), and Heroku to perform daily full backups of all data stored in the cloud. CSP backups are performed using the CSP’s automated backup tool.

Backups are stored in a secure remote location at a sufficient distance to escape damage from a disaster at the main site of processing. Data will be retained for thirty (30) days.

Backups are tested annually by the Engineering team to ensure that they can be restored and relied upon in an emergency. As part of testing, management determines their ability to meet the company's restoration time requirements.

Monitoring Policy

Event Monitoring Policy

FinGoal implements comprehensive auditing and monitoring controls to identify and capture the following events:

- All authentication and authorization activities by all users and their associated accounts (e.g., successful and unsuccessful login attempts)
- Any access to or creation, modification, or deletion of Sensitive or Customer data
- All actions taken by privileged users
- Malicious activity

FinGoal monitors system components to capture these events with specialized software such as File Integrity Monitoring (FIM), Host-based Intrusion Detection Systems (HIDS), and/or change detection software programs. Notifications are set up to alert authorized Engineering personnel if immediate action needs to be taken.

The CTO is responsible for monitoring and communicating changes and events.

Performance and Utilization Monitoring Policy

FinGoal monitors system components (e.g., servers) for appropriate performance and utilization by taking the following measures:

- **Process monitoring:** FinGoal monitors all critical processes and provides alerting and notification measures when processes fail.
- **Network interface monitoring:** FinGoal monitors the overall health and status of the network interface.
- **CPU utilization:** FinGoal identifies current, real-time capacity of the central processing unit (CPU) and sends alerts and notifications if capacity is over limits and/or assets are underutilized.
- **Memory utilization:** FinGoal identifies current, real-time memory usage and sends alerts and notifications if memory usage is high and/or if memory availability is low.
- **Disk utilization:** FinGoal identifies current, real-time disk space and sends alerts and notifications if disk space is low.

Logging and Reporting Policy

Along with capturing all necessary events described in the Event Monitoring Policy, FinGoal implements protocols to log, store, and review all required events and their associated attributes as necessary.

Logging

FinGoal uses capturing and forwarding protocols (e.g., Syslog) and/or specialized software applications or other technology as necessary to protect the confidentiality, integrity, and availability of audit trails and their respective log reports that are produced by monitoring activities.

Review

The CTO reviews all applicable user permissions and related output (e.g., log reports) to identify any issues or concerns and report them immediately to appropriate personnel.

Reporting

Any anomalies, such as unauthorized configuration changes in the logs, are escalated in accordance with the Incident Management Policy.

Network and System Security Policy

Data Handling Policy

Types of Data

The following types of data are stored, processed, and/or transmitted on system components that are owned, operated, maintained, and controlled by FinGoal:

- **Sensitive:** Applies to the most sensitive business information, to which access is strictly limited (e.g., passwords, encryption keys)
- **Confidential:** Applies to less sensitive business information, which is intended for use solely by the Company and/or its customers (e.g., Personally Identifiable Information (PII), balance sheets, income statements, internal market research, audit reports)
- **Public:** Applies to all other information that does not clearly fit into the above classifications

Retention

FinGoal retains Sensitive and Confidential data only for as long as necessary to fulfill its purposes unless otherwise required by law or to meet legal and customer contractual obligations. To support compliance with these obligations, the Chief Technology Officer (CTO) or equivalent role reviews FinGoal's data retention practices on an annual basis.

Disposal

FinGoal securely disposes of Sensitive and Confidential data following defined processes once it is no longer necessary for legal, regulatory, or business requirements or it has reached the end of its retention period.

The following methods are used for both hard copy and electronic data:

- Purging and deleting data from all system components using a secure wipe program in accordance with industry-accepted standards for secure deletion (e.g., degaussing)
- Destroying any cardholder data that is in a hard copy format (e.g., cross-shredding)

For electronic media stored on system components that are no longer in use, data is disposed of using one of the following methods:

- Disintegration
- Shredding by a disk grinding device
- Incineration by a licensed incinerator
- Pulverization

Instances of customer data disposal are tracked via a ticketing system to document the steps taken to complete the removal.

Information Security Policy

FinGoal maintains reasonable technical, organizational, and physical security measures to protect the security of Sensitive and Confidential data in transit, at rest, and in storage from unauthorized access or unlawful disclosure.

Critical security controls include, but are not limited to, the following:

- **Encryption in transit:** Sensitive and Confidential data transfers are sent via a secure transfer system that is transport layer security (TLS) 1.2 or higher.
- **Encryption at rest:** All FinGoal servers, workstations, and laptops use advanced encryption standard (AES) 256 disk encryption.
- **Outbound files:** A secure file transfer platform is used to transfer files outside of the FinGoal network.
- **Inbound files:** During transfer, all files sent into the FinGoal network are verified that they are free of corruption and that the files originated from a known source.

- **Database:** Company application databases that are externally accessible by web traffic are encrypted and provide a level of identification security using an application-specific protocol such as HTTPS. Sensitive and Confidential data in FinGoal databases is also encrypted from the customer's side before being inserted into the database.
- **Data segregation:** Sensitive and Confidential data remains in either the on-premises deployment of FinGoal's products or secure cloud environments.
- **Data storage:** Sensitive and Confidential data is only stored in approved systems, databases, and endpoints (e.g., laptops).
- **Cloud storage:** Secure and Confidential data is stored in a secure, dedicated cloud environment behind a firewall.
- **Production and test environments:** FinGoal sanitizes all production data before use in non-production environments, as applicable.
- **Incident management:** FinGoal maintains a process for identifying, managing, and resolving privacy incidents in accordance with the FinGoal Incident Management Policy.

Pandemic Response Planning Policy

This policy is intended for companies that do not meet the definition of critical infrastructure as defined by the US Federal Government. This type of organization may be requested by public health officials to close their offices to non-essential personnel or completely during a pandemic to lower the immediate risk and limit the spread of the disease. Many companies would run out of cash and be forced to go out of business after several weeks of everyone not working. Therefore, developing a response plan in advance that addresses who can work remotely, how they will work and identifies what other issues may be faced will help the organization survive at a time when most people will be concerned about themselves and their families.

Disasters typically happen in one geographic area. A hurricane or earthquake can cause massive damage in one area, yet the worst damage is usually contained within a few hundred miles. A global pandemic, such as the 1918 influenza outbreak which infected 1/3 of the world's population, cannot be dealt with by failing over to a backup data center. Therefore, additional planning steps for IT architecture, situational awareness, employee training and other preparations are required.

Purpose

This policy directs planning, preparation and exercises for pandemic disease outbreak over and above the normal business continuity and disaster recovery planning process. The objective is to address the reality that pandemic events can create personnel and technology issues outside the scope of the traditional Disaster Recovery/Business Continuity Planning process as potentially some if not the entire workforce may be unable to come to work for health or personal reasons.

Scope

The planning process will include personnel involved in the business continuity and disaster recovery process, enterprise architects and senior management of FinGoal. During the implementation of the plan, all employees and contractors will need to undergo training before and during a pandemic disease outbreak.

Policy

FinGoal will authorize, develop and maintain a Pandemic Response Plan addressing the following areas:

- □ The Pandemic Response Plan leadership will be identified as a small team which will oversee the creation and updates of the plan. The leadership will also be responsible for developing internal expertise on the transmission of diseases and other areas such as second wave phenomenon to guide planning and response efforts. However, as with any other critical position, the leadership must have trained alternates that can execute the plan should the leadership become unavailable due to illness.
- □ The creation of a communications plan before and during an outbreak that accounts for congested telecommunications services.
- □ An alert system based on monitoring of the World Health Organization (WHO), the Centers for Disease Control (CDC) and other Federal, State and Local sources of information on the risk of a pandemic disease outbreak.
- □ A predefined set of emergency policies that will preempt normal FinGoal policies for the duration of a declared pandemic. These emergency policies are to be organized into different levels of response that match the level of business disruption expected from a possible pandemic disease outbreak within the community. These policies should address all tasks critical to the continuation of the company including:

□ How people will be paid

□ Where people will work – including staying home with or bringing kids to work

□ How people will accomplish their tasks if they cannot get to the office

□ What work will be suspended during the pandemic

□ Communication plan and cadence throughout the pandemic

□ Alternate means to communicate during the pandemic

□ What operational procedures may need to be altered, amended, or suspended, such as those over facilities, visitors, and non-essential activities and events

□ A set of indicators to management that will aid them in selecting an appropriate level of response bringing into effect the related policies discussed in section 4.4—for the organization. There should be a graduated level of response related to the WHO pandemic alert level or other authoritative indicators of a disease outbreak.

□ An employee training process covering personal protection including:

□ Identifying and broadly communicating the symptoms of exposure

□ The concept of disease clusters in daycares, schools or other large gatherings

□ Basic prevention - limiting contact closer than 6 feet, cover your cough, hand washing

□ When to stay home along with encouragement to do so

□ Avoiding travel to all areas with high infection rates

□ A process for the identification of employees with first responders or medical personnel in their household. These people, along with single parents, have a higher likelihood of unavailability due to illness or child care issues.

□ A process to identify key personnel for each critical business function and transition their duties to others in the event they become ill or unable to perform their respective duties.

□ A list of supplies to be kept on hand or pre-contracted for supply, such as face masks, hand sanitizer, fuel, food and water.

IT related issues:

□ Ensure enterprise architects are including pandemic contingency in planning

□ Verification of the ability for significantly increased telecommuting including bandwidth, VPN concentrator capacity/licensing, ability to offer voice over IP and laptop/remote desktop availability

□ Increased use of virtual meeting tools that facilitate video conference and desktop sharing capabilities

- □ Identify what tasks cannot be done remotely
- □ Pre-negotiated arrangements with key vendors in the event current licensing will not meet this change in work force habits
- □ Determine if any IT colleagues need to remain onsite to support critical operations
- □ Plan for how customers will interact with the organization in different ways
- □ Expectations concerning printing work documents on personal printers
- □ Expectations about sending work emails and documents to personal email accounts
- □ The creation of exercises to test the plan in advance.
- □ Performing a retrospective review to identify and solve for issues encountered in the test
- □ The process and frequency of plan updates and review at least annually with appropriate approvals or sign-off from organizational leadership or oversight.
- □ Guidance for auditors indicating that any review of the business continuity plan or enterprise architecture should assess whether they appropriately address the FinGoal Pandemic Response Plan.

People Security Policy

Employee Confidentiality Agreements

Employees are required to read and accept the terms of a confidentiality agreement upon hire that states they are prohibited from disclosing any company data from the systems and system components to which they have access. FinGoal ensures that these agreements comply with all applicable laws. The organization will not grant an employee access to any FinGoal assets without obtaining the employee’s verified acknowledgment of the agreement.

Background Check Policy

FinGoal uses either an approved background check vendor or defined reference checks to perform background checks on individuals prior to their start date.

Security Awareness Training

All employees within FinGoal must undergo security awareness training within thirty (30) days of hire and at least annually thereafter.

The training accomplishes the following:

- Ensure employees are aware of significant security issues that pose a credible threat to the organization, its network infrastructure, and its supporting system resources
- Establish a comprehensive framework that effectively addresses the core components of security awareness, training, and education
- Provide subject matter directly related to the safety and security of specific system components, especially those to which all users have access
- Communicate the necessary response and resolution measures if employees suspect a security event or incident

Management monitors completion of security awareness training and follows up with employees who have not complied with the above requirement.

Performance

As part of maintaining information security standards, managers are required to complete performance appraisals for direct reports at least annually.

Physical Security Policy

FinGoal has a distributed work from home policy and a central office location in Lafayette, Colorado. The purpose of our physical security policy is to provide a framework and procedures for identifying and dealing with security risks facing FinGoal and its employees. This policy will allow the company, in as far as is reasonably practicable, to ensure the safety and security of our physical locations and the people using them.

Roles and Responsibilities

Management

It is essential that adequate resources are made available for managing the risk arising from security-related issues within the company. It is important that all personnel involved in implementing this policy are competent, trained and aware of their responsibilities.

Office Security

FinGoal's physical office must always be locked when unattended. The office space in general is protected by Proximity, and only authorized FinGoal employees are able to access the space during off-business hours. A key code is used to keep the internal door locked. This code should not be distributed to anyone outside of the FinGoal organization.

Cameras

Cameras are used throughout the interior and exterior of the office space.

Privacy Impact Assessment Policy

Conducting a Privacy Impact Assessment (PIA) ensures compliance with laws and regulations governing privacy and demonstrates FinGoal's commitment to protect the privacy of any personal information we collect, store, retrieve, use and share. It is a comprehensive analysis of how FinGoal's information systems and collections handle Personally Identifiable Information (PII). The objective of the PIA is to systematically identify the risks and potential effects of collecting, maintaining, and disseminating PII and to evaluate alternative processes for handling information to mitigate potential privacy risks.

Statement on Data Privacy and Ownership

Privacy is a fundamental human right. At FinGoal, it's also a core value. Users trust the financial brands served by FinGoal with private data. FinGoal designs products and services to protect user privacy and give users control over their information. It's not always easy. But that's the kind of innovation FinGoal is committed to delivering. FinGoal believes that, at a minimum, data supplied to FinGoal belongs to the supplier of that data. Ideally, when this data supply chain originates from an end-user, that end-user is the owner of that data. Typically, end-user data is provided to FinGoal through a financial brand or partner who has a direct relationship with the end-user. FinGoal is not in the position to declare whether the end-user or the partner is the owner of that data. Definitively, FinGoal is not the owner. Data derived from aggregated data sets by FinGoal with the consent of the end-user, by default, belongs to FinGoal unless otherwise stated.

Scope

All FinGoal employees, contractors, and temporary workers with access to data persisted by FinGoal.

Policy

A new PIA should be completed by a member of FinGoal's leadership team when any of the following activities occur:

- □ New technologies or systems are developed or integrated that handle or collect PII.
- □ PII handling systems are revised.
- □ An electronic collection of information in identifiable form is requested.
- □ An update is made to the FinGoal Data Classification Policy.

Drafting a PIA

New PIAs for FinGoal must address the following concerns:

- □ Does the project or system collect, maintain, retrieve or share any data that can be used to directly or indirectly identify an individual?
- □ Does this project or system retrieve information using a personal identifier?

If the answer to either of the above questions is yes, the PIA's drafter must include the specific use case for requiring PII in the system. The leadership team is responsible for reviewing PIAs and determining if the request for PII is warranted, and determining if any alternatives may be proposed.

FinGoal’s PIA

FinGoal APIs and the applications analyze user credit and debit transactions to generate actionable insights on transactions to help financial brands better target and serve their users & account holders.

Use of PII

FinGoal may consume, persist, and transmit PII in a variety of forms, including:

- □ Transactions
- □ May include first and last names, names of family or friends, location data, sensitive health data, etc, on a case-by-case basis.
- □ Demographic data
- □ Location data
- □ Account balance data

FinGoal aggregates this data from several clients and partners. The data is collected and persisted to enable FinGoal’s machine learning systems and human curators to provide high quality, personalized advice and insight.

PII at FinGoal is collected from clients, and the amount collected and nature of the PII is dependent on the client and how much PII they collect and transmit to the core API.

During ordinary operation, PII is collected with anonymous identifiers and all transaction and account data is anonymized before being transmitted to anyone other than the data’s owner.

Data Attributes

All PII within the system is persisted in order to make FinGoal’s output more relevant. The value generated by FinGoal’s machine learning algorithms is shared back with the client, and used to improve the engine as a whole.

Sharing Practices

FinGoal does not share client or end-user data with third parties. If an exception is to be made, it must first be approved by the client, end-user, and the FinGoal leadership team.

Notice to Individuals to Decline/Consent Use

FinGoal does not aggregate personal information without an end-user’s express consent. Users must authenticate with their banking provider and follow clear steps to allow FinGoal to gain access to their personally identifiable financial information. FinGoal does not attempt to gather more PII about end-users without their consent.

Access to Data

End-user personally identifiable financial data is persisted in FinGoal’s systems until the end-user ceases utilizing the application for a 12-month period or expressly requests that their data be removed.

FinGoal clients have access to all the data they have aggregated through the FinGoal platform; end-users have access only to their personal data.

FinGoal’s human advice curators have access to anonymized transaction records, and all PII is redacted before being put before them. Only FinGoal’s database administrators, who are on the leadership team, have direct access to the production database, and even then, administrators may only access a portion of the data without obtaining special access.

FinGoal relies on Least Privilege and RBAC principles when governing data access for end-users, clients, employees, contractors, administrators, and executives.

Risk Management Policy

FinGoal has designed a risk assessment program to assess the organization’s enterprise-level risk at least annually or upon significant changes to the environment.

As part of the risk assessment process, FinGoal will do the following:

- Specify FinGoal’s objectives and identify and assess risks related to these objectives.
- Identify and assess threats to and vulnerabilities in systems and service (the latter through changes to service commitments)
- Determine the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system relative to the information it processes, stores, or transmits

- Integrate risk assessment results and risk management decisions with the organization, its mission, and/or its business process perspectives via system-level risk assessments
- Document risk assessment results in the organization’s risk registry and respond to the results in accordance with FinGoal's risk tolerance
- Disseminate risk assessment results to key stakeholders
- Update the risk assessment when there are significant changes to the system, its operating environment, or other conditions that may impact the security or privacy of the system
- Identify and assess potential fraud and its potential impact on the organization’s objectives
- Ensure management selects and develops manual and technical general control activities to assist in mitigating risks

Security Organization and Management Policy

Security Roles and Responsibilities

FinGoal has an organizational structure that establishes, approves, implements, and monitors adherence to an Information Security Program through clear lines of authority and responsibilities.

Risk Committee

FinGoal has appointed a Risk Committee consisting of internal personnel and at least one independent member (or one member independent of the control function). The Risk Committee has oversight responsibilities related to internal security controls, which are detailed in the Risk Committee Charter.

Responsibilities include the following:

- Approving and monitoring adherence to this policy
- Ensuring data handling responsibilities are assigned, documented, and communicated
- Performing the annual risk assessment

The Risk Committee meets at least quarterly and maintains formal meeting minutes.

Personnel

The following personnel are responsible for overseeing and implementing security and data protection practices throughout FinGoal:

- **CTO:** Responsibilities include providing overall direction, leadership, and support on methods and tools for secure storage, retention, and disposal of Confidential and Sensitive data.
- **Systems Administrators:** Responsibilities include implementing the baseline configuration standards for all in-scope system components as well as managing user access to FinGoal information systems that contain Confidential and Sensitive data. (For data classifications, see Types of Data.)
- **End Users (Employees, Consultants):** Responsibilities include adhering to the organization's data protection policies, procedures, and practices and reporting instances of non-compliance to senior authorities, especially instances by other users.
- **Vendors (includes Contractors and other Third Parties):** Responsibilities include all those applicable to end users. In addition, vendors, contractors, and third parties are responsible for:
    - Avoiding any measure to alter such standards that protect customer data;
    - Completing due diligence and ongoing monitoring assessments per the requirements set forth in the Vendor Management Policy; and
    - Immediately notifying FinGoal of any policy violations involving customer data.

Every end user and vendor is responsible for identifying and mitigating risks associated with the protection of Confidential information and must comply with all the policies within this Information Security Policy.

Policy Review

The CTO is responsible for reviewing FinGoal's policies and procedures on at least an annual basis to ensure they remain accurate.

Vendor Management Policy

FinGoal requires vendors to maintain their own security practices and procedures and to abide by FinGoal's security policies.

New Vendors

Using a defined process, FinGoal management assesses a potential vendor to evaluate its criticality and riskiness. Relevant assessment criteria may include but is not limited to:

- The vendor's expertise, experience, and reputation
- The nature and necessity of the service
- Whether a vendor needs access to Sensitive or Confidential data
- The vendor's security infrastructure
- The vendor's level of contact with customers

A vendor's criticality rating determines the level and intensity of initial due diligence and ongoing monitoring. It also facilitates management's ability to appropriately manage process dependencies on suppliers and quickly identify which vendors have access to Sensitive or Confidential data.

Criticality Rating

Possible vendor criticality ratings are defined below.

Critical

- Daily operations critically depend on the service.
- Service failure or significant impairments would halt business processes.
- Supplier provides a service critical to developing, supporting, and securing the company software product.

High

- Daily operations significantly depend on the service.
- Service failure or significant impairments would seriously disrupt business processes.
- Supplier provides a service that is significantly important to developing, supporting, and securing the company software product.

Medium

- Daily operations regularly use the service but do not depend on it.
- Service failure or significant impairments would impair but not seriously disrupt business processes.
- Supplier service is used for developing, supporting, and securing the company software product, but it is not a critical function.

Low

- Operations regularly use the service but unevenly (i.e., not every day or not every user).
- Service failure or significant impairments would present challenges to operations but would not disrupt business processes.
- Supplier service is used for developing, supporting, and securing the company software product, but it is not an essential function.

Vendor Review

FinGoal collects and reviews a compliance report at least annually on all vendors rated critical or high risk. The review is documented and any exceptions or deviations noted in the reports are evaluated to determine their impact on the service.

Vulnerability Management Policy

FinGoal's vulnerability management program ensures the confidentiality, integrity, and availability (CIA) of the organization's information systems landscape, which includes all critical system resources.

The FinGoal vulnerability management program addresses vulnerabilities and threats through remediation and control implementation. These terms are defined as follows:

- **Vulnerabilities**: Software flaws or misconfigurations that may weaken the security of an organization's system
- **Threats:** Capabilities or methods of attack developed by malicious entities to exploit vulnerabilities and harm a computer system or network. Potential threats also include insider threats

- **Remediation:** Means of addressing or resolving vulnerabilities and threats
- **Control implementation:** The use of defined scanning and testing procedures to identify, communicate, and address vulnerabilities and threats

Chief components of the program include the following:

- **Configuration standards:** FinGoal establishes a secure information security baseline by provisioning, hardening, securing, and locking down all critical system resources through continuous monitoring and security patches. (See Information Security Policy.)
- **Network architecture:** FinGoal develops secure network architecture and secure segmentation to prevent vulnerabilities.
- **Network scanning and monitoring:** FinGoal follows internal and external vulnerability scanning procedures and conducts network layer and application layer penetration tests to manage vulnerabilities.

Vulnerabilities will be categorized by severity based on the following criteria:

- **Impact:** The possible disruption to systems and business operations
- **Likelihood:** The ease in which a vulnerability may be exploited
- **Compensating controls:** The availability of network- or host-based methods of mitigation

The classification and prioritization of vulnerabilities are based on the Open Web Application Security Project (OWASP) Risk Rating Methodology. Separate Impact and Likelihood scores are assigned to the identified vulnerability. The combined scores result in an overall severity score for the vulnerability, indicating its prioritization for remediation.

Network Segmentation

FinGoal segments its network to prevent direct or unauthorized connections between an external network and its information systems – and in particular between an external network and Confidential data in cloud environments. Segmentation is established through the following means:

- Demilitarized zones (DMZ) that logically separate FinGoal's systems and data from untrusted external networks
- Security tools that isolate subnetworks and security groups (e.g., customer environments) and prohibit connection except through monitored interfaces

Vulnerability Scanning

FinGoal performs internal and/or external vulnerability scans to test in-scope systems. These scans are initiated under 2 conditions:

1. New code is released to a branch in a Github repository that deploys to a cloud hosted or otherwise deployed FinGoal application.
2. Github discovers a new vulnerability, uploads it to their registry, and one or more of FinGoal's deployed branches possesses a dependency which has the vulnerability.

These reports are shared with authorized Engineering personnel.

Penetration Testing

Independent third-party penetration tests are conducted at least annually on any systems that use Confidential data or that have been assigned a critical risk rating in order to identify security vulnerabilities. Before initiating each penetration test, FinGoal documents in-scope assets in an asset inventory. Management, in consultation with Security teams and applicable Product personnel, views the test results and addresses and remediates any vulnerabilities based on risk level.

Vulnerability Remediation Procedure

Once an employee has identified a critical or zero-day vulnerability, they report the vulnerability immediately to the CTO, who is responsible for carrying out this procedure for each identified vulnerability.

- □ Develop a vulnerability analysis. Document the following details about the vulnerability:
    - Description/Nature of the vulnerability
    - System(s) impacted
    - Risk rating based on the potential impact, the likelihood of exploitation, and any existing controls that may reduce the risk:
        - **Critical:** Daily operations absolutely depend on the system affected by the vulnerability. Failure or significant impairments would halt business operations.

        - **High:** Daily operations significantly depend on the system affected by the vulnerability. Failure or significant impairments would seriously disrupt business operations.
        - **Medium:** Daily operations regularly incorporate but do not depend on the system. Failure or significant impairments would noticeably affect but not prevent or seriously disrupt business operations.
        - **Low:** Operations use the service regularly but unevenly. Failure or significant impairments would present challenges to but not disrupt business practices.
    - Any suggested controls that may be implemented to address the vulnerability

- □ Determine the remediation timeline based on the risk rating:

    - **Critical:** Immediately to 7 days from identification
    - **High:** Within 14 days of identification
    - **Medium and Low:** Within 30 days of identification

Patch Management Policy

Effective patch management and system updates help ensure the confidentiality, integrity, and availability of systems from new exploits, vulnerabilities, and other security threats. All necessary system patches and system updates to FinGoal's underlying infrastructure are obtained from the software vendor and/or other trusted third parties:

- Vendor websites and email alerts
- Vendor mailing lists, newsletters, and additional support channels for patches and security
- Third-party websites and email alerts
- Third-party mailing lists
- Approved online forums and discussion panels

All necessary system patches and system updates to FinGoal's underlying infrastructure are obtained and deployed at least monthly. The specific timeline for applying patches depends on the severity level of the vulnerability for each system component. FinGoal uses the following timelines for patch management based on severity level:

- **Critical:** Immediately to 7 days from identification
- **High:** Within 14 days of identification

- **Medium and Low:** Within 30 days of identification

Patches fixing highly critical or zero-day vulnerabilities are escalated and applied as soon as possible. The CTO considers the following factors to determine when to apply the patch:

- The relative importance of the vulnerable systems
- The relative severity of each vulnerability
- The operational risks of patching without first testing
- Whether there is a viable option to mitigate the vulnerability through an alternative method, at least until patches are fully deployed and operational

Antivirus Protection Policy

FinGoal has antivirus (AV) solutions to detect malicious code and malware. AV is deployed on all of the following applicable system components in its underlying infrastructure: laptops.

The AV meets the following criteria:

- The most current version available from the vendor
- Enabled for automatic updates
- Configured for conducting periodic scans at least monthly
- Capable of removing all known types of malicious software

All AV solutions will generate logs for monitoring and alerting IT personnel about infected machines. Because strong and comprehensive malware measures are not just limited to the use of AV, additional tools are to be employed as necessary for eliminating all other associated threats.

Change Control

Date	Version	Change(s)	Reason for Change(s)	Change(s) Made By
2020-06-01	1	Initial Version	Creation	Jack Ryan
2021-07-01	1.1	Convert to Notion	Ease of Management	Jack Ryan
2022-04-21	1.2	Review of Policy and minor edits	Clarity	Carolyn Nohe
2023-04-20	2	Addition of Thoropass Policies	Preparation for SOC 2	Jack Ryan
2023-06-01	2.1	Merge of Thoropass and Additional Policies. Change to Alphabetical Order of sections w/ subsections listed in ToC.	Thoropass was missing several policies that FinGoal uses. Alphabetical order is easier for the reader.	Jack Ryan

TITLE	Information Security Policy
FILE NAME	Information Security Policy.pdf
TIMESTAMP	06/22/2023 at 18:52:37
VERSION	V-2
OWNER	John Ryan
APPROVER	John Ryan

Document History

V-2	06/22/2023 at 18:52:37	Changed by: John Ryan jack@fingoal.com Comments: Updated scanning policy to reflect GH Dependabot's scanning cadence rather than daily scanning.
V-1	04/20/2023 at 15:02:13	Changed by: John Ryan jack@fingoal.com Comments: Edited initial draft for clarity's sake; informationally, the only change I've made is that FinGoal's staging environments do not automatically initiate releases to the production environment; we still subject those to an auxiliary review and I don't think we'll change that element of our process within the year.