Information Security Policies

fpPATHFINDER

PO Box 1554,
Farmington, Connecticut, 06034
www.fpPathfinder.com

CONFIDENTIAL

DOCUMENT VERSION 1.0

PUBLISHED: OCTOBER 2022

<table>
<tr><td colspan="5">This Policy has been approved according to the chart shown below. Any deviation from this policy will require the written approval the CEO.</td></tr>
<tr><th>Published Date</th><th>Rev #</th><th>Changes Made</th><th>Author(s)</th><th>Approver(s)</th></tr>
<tr><td>October 2022</td><td>1</td><td>First Instance</td><td>Mike Treacy/Christina Stokes</td><td>Stacia Waren/Michael Lecours</td></tr>
</table>

Table of Contents

Information Security Terms and Conditions of Employment Policy

1. Introduction

fpPathfinder takes the subject of information security very seriously, including confidential and/or customer information as well as business-sensitive internal records and correspondence.

As an employee, contractor, or partner, you will be expected to review, understand, acknowledge, and comply fully with any and all information security policies, procedures, and standards. This section outlines some of the key security provisions of fpPathfinder's security policy. Everyone is required to read these statements, and all policies published by fpPathfinder, and acknowledge their understanding in writing.

2. General Provisions

Please read the following general provisions carefully.

1. I acknowledge that my use of a company computer and communications systems may be monitored
2. I acknowledge that I am responsible for safeguarding my password and any other authentication information provided to me
3. I will not use any account and password other than the one assigned to me (e.g., another user's credentials)
4. I will not attempt to access any computer system to which I have not been given access
5. I will not attempt to bypass or subvert system security controls without specific, written management approval
6. I will protect confidential and customer data, including both electronic and paper copies
7. I will label any confidential material that I create and/or ensure that it is located in a repository where protection level is unambiguous
8. I will not send confidential or customer information via unsecured channels (e.g., email)
9. I will safely store confidential printed materials and ensure they are destroyed when no longer needed
10. I will not leave my computer unlocked when unattended
11. I will read and agree to abide by all published organizational security policies and procedures
12. I will inform my manager immediately if I observe any behavior or situations that could constitute a breach of security
13. I will protect mobile devices such as laptops and phones when they are off premises
14. I will comply with all legal, statutory and/or applicable contractual obligations
15. If I have any questions about information security policy or procedures, or I do not fully understand how to comply with them, I will discuss this with my manager immediately
16. On leaving the organization, I will inform my manager prior to departure of any important information held in my account.

3. Declaration

I have read the above statements and, by affixing my signature below, agree to comply fully. I hereby state that I have read and will abide by all applicable information security policies and procedures and agree to abide by any future policies and procedures published by the organization in the future.

Name: Stacia Waren

Signature: Stacia Waren

Date: 11/1/2022

Information Security Roles Responsibilities and Authorities

1. Introduction

fpPathfinder treats the security of its information assets very seriously and has established an Information Security Management System (ISMS) which conforms (to the extent applicable) to the ISO/IEC 27001 international standard for information security. One of the key attributes of an effective ISMS is a clear allocation of roles, each with defined responsibilities and authorities. Each of these roles needs to be allocated to specific individuals or groups within the organization.

By ensuring that roles, responsibilities and authorities are clearly defined, we will be in a good position to prevent many incidents from happening and to react effectively and appropriately if and when they do.

2. General Provisions

2.1 Information Security Roles

Within the ISMS the following major roles need to be defined and allocated:

- Information Security Committee
- Chief Information Security Officer

The specific responsibilities and authorities of each of these roles are set out in later sections of this document. There are also particular information security responsibilities that must be carried out by existing roles within the organization, and these are also set out in summary within this document. These roles are:

- Department Managers
- IT Technicians
- IT Users

In general, responsibilities that apply to all employees, contractors, and other interested parties are set out within the relevant organizational policies.

2.2 Organization Structure

The relevant groups are as follows:

- Information Security Committee – Michael Lecours, Stacia Waren, and Mike Treacy
- Chief Information Security Officer – Michael Lecours

2.3 ISMS Responsibility Matrix

Overall responsibility for the management of the various sections of the ISO/IEC 27001 standard is shown in the following RACI table. This defines the type of responsibility of each role in each area according to whether the listed role is:

R= Responsible A= Accountable C= Consulted I= Informed

ISO/IEC 27001 Topics	Information Security Committee	CISO
Context	R	I
Leadership	R	I
Planning	A/C	R
Support	A/C	R
Operation	A/C	R
Performance evaluation	A/C	R
Improvement	A/C	R
Annex A Controls	A/C	R

Table 1 - RACI chart

These responsibilities are expanded on further within the rest of this document.

3. Specific Role Responsibilities

This section details the specific ***information security*** responsibilities and authorities of each role within fpPathfinder's organization structure. It does not include any other types of responsibility (e.g. managerial, technical) and should not be taken as a full job description.

3.1 Information Security Committee

The Information Security Committee oversees the operation of the ISMS as a representative of top management within fpPathfinder and has overall responsibility for its effectiveness.

Members

The group is made up of members of the top management team and will as a minimum include representatives in the following areas:

- Operations
- Finance
- IT
- CISO

Further members may be nominated by existing members on an as-needed basis.

Responsibilities

The Information Security Committee has the following responsibilities:

- Establish and maintain the ISMS policy, objectives and plans
- Communicate the importance of meeting the objectives and the need for continual improvement throughout the organization
- Maintain an awareness of business needs and major changes

- Ensure that information security requirements are determined and are met with the aim of minimizing risk and maintaining effective controls
- Determine and provide resources to plan, implement, monitor, review and improve information security and management (e.g., recruit appropriate staff, manage staff turnover)
- Oversee the management of risks to the organization
- Conduct management reviews of information security, at planned intervals (at least annually), to ensure continuing suitability, adequacy and effectiveness
- Select auditors and ensure that internal audits are conducted in an objective and impartial manner
- Maintain relationships with appropriate special interest groups
- Establish a continual improvement policy with respect to information security for fpPathfinder
- Review major information security incidents
- Ensure that arrangements that involve external organizations having access to information systems and services are based on a formal agreement that defines all necessary security requirements
- If a breach occurs, follow the incident response procedure and contact the relevant authorities, if necessary

Authorities

The Information Security Committee has the authority to:

- Approve significant expenditure on information security-related matters
- Recruit additional resources for the management of information security
- Approve high-level policies for information security
- Initiate high-level incident management actions

3.2 Chief Information Security Officer

The Chief Information Security Officer is the primary role with a dedicated focus on information security and related issues. Note that, as needed, managed security service providers and/or contract personnel may be employed to support areas of information security operational responsibility as deemed appropriate by fpPathfinder management.

Responsibilities

The Chief Information Security Officer has the following responsibilities:

- Reporting to the Information Security Committee on all security related matters on a regular and ad-hoc basis when required
- Communicate the information security policy to all relevant interested parties where appropriate
- Implement the requirements of the information security policy
- Manage risks associated with access to the service or systems
- Ensure that security controls are in place and documented
- Quantify and monitor the types, volumes and impacts of security incidents and malfunctions
- Define improvement plans and targets for the financial year
- Monitor achievement against targets
- Establish and maintain a continual improvement action list
- Report on improvement activities
- Identify and manage information security incidents according to a process
- Attend management review meetings on a regular basis

Authorities

The Chief Information Security Officer has the authority to:

- Declare information security incidents
- Review the operation of controls within all business areas
- Advise management on the selection of controls and mitigation of risks

4. Other Roles with Information Security Responsibilities

There are a number of other roles within the organization which, whilst not solely dedicated to information security, have relevant responsibilities and authorities.

4.1 Department Managers

Department Managers may be heads or supervisors of operational units within the organization.

Responsibilities

A Department Manager has the following responsibilities:

- Review and manage employee competencies and training needs to enable them to perform their role effectively within the information security area
- Ensure that employees are aware of the relevance and importance of their activities and how they contribute to the achievement of information security objectives

Authorities

A Department Manager has the authority to:

- Arrange training and awareness activities for the employees under their direction, within budget constraints
- Take action to prevent an information security incident from occurring or escalating, where possible

4.2 IT Technicians

Due to the often technical nature of information security issues, IT technicians have an important part to play in the ISMS.

Responsibilities

IT Technicians generally have the following responsibilities:

- Operation of processes such as incident and change management
- Provision of technical expertise in matters of information security
- Implementation of technical controls
- System administration e.g., user creation, backups
- Security monitoring e.g., network intrusions

Authorities

An IT Technician has the authority to:

- Take action to prevent an information security incident from occurring or escalating, where possible

4.3 IT Users

The responsibilities of IT users are defined in a variety of organization-wide policies and are only summarized in brief below.

Responsibilities

An IT user has the following main responsibilities:

- Ensure they are aware of and comply with all information security policies of the organization relevant to their business role
- Report any actual or potential security breaches
- Contribute to risk assessment activities where required

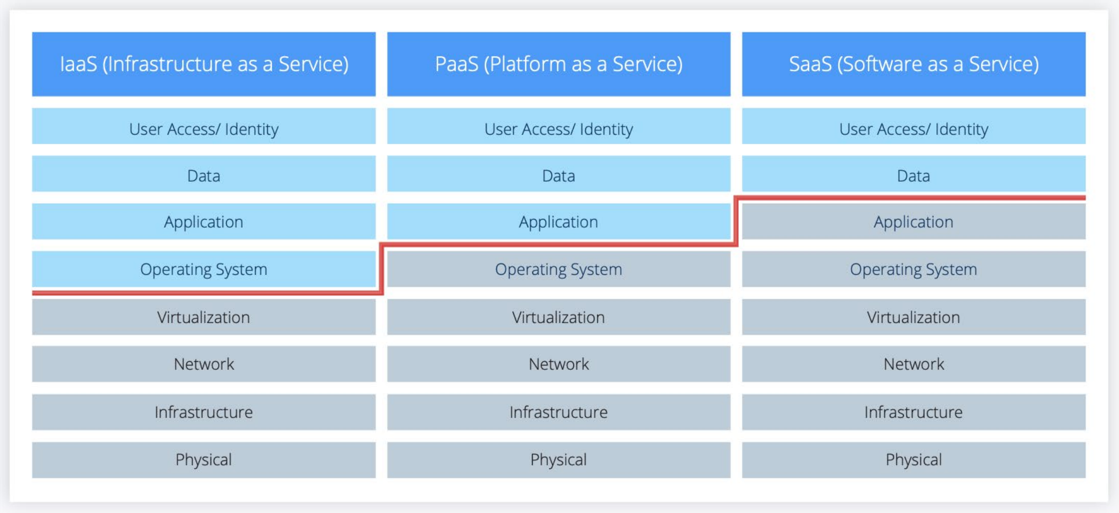
Authorities

An IT user has the authority to:

- Take action to prevent an information security incident from occurring or escalating, where possible

5. Shared Responsibility with Cloud Provider

fpPathfinder follows this shared responsibility model:



IaaS (Infrastructure as a Service)	PaaS (Platform as a Service)	SaaS (Software as a Service)
User Access/ Identity	User Access/ Identity	User Access/ Identity
Data	Data	Data
Application	Application	Application
Operating System	Operating System	Operating System
Virtualization	Virtualization	Virtualization
Network	Network	Network
Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical

🟦 Blue - Cloud Client/Consumer Security Responsibility
⬜ Grey - Cloud Service Provider Security Responsibility

Fig 1. Shared Security Responsibility model

6. Exceptions

This policy applies to all employees and contractors. Those found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

7. Responsibilities

It is the responsibility of all contractors, employees, and management to ensure that this policy is followed.

Access Control Policy

1. Overview

The control of access to fpPathfinder's information assets is a fundamental part of our defense in depth strategy to information security.

User access rights must be reviewed at regular intervals (quarterly) to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

2. User Registration and Deregistration

For environments storing, processing, or transmitting confidential or customer information (i.e., information of the highest classification), the following requirements apply.

A request for access to systems must be submitted in writing to the CEO, Michael Lecours, for approval. All requests will be processed according to a formal procedure that ensures that appropriate security checks are carried out and correct authorization is obtained prior to account creation. All access right additions, changes and removals will be noted. Where feasible, the principle of segregation of duties will apply so that the creation of the account and the assignment of permissions are performed by different people.

Each account will have a unique username that is not shared with any other user and is associated with a specific individual (i.e., not a role or job title). Generic accounts i.e., single accounts to be used by a group of people should not be created unless they are non-optional (i.e., "root", "Administrator", or other special-purpose accounts).

Initial passwords must be strong and securely delivered; users must be required to change the password on first use of the account.

In exceptional circumstances where there is perceived to be a risk that the employee may take action that may harm the organization prior to or upon termination, a request to remove access may be approved and actioned in advance of notice of termination being given. This precaution should especially apply in the case where the individual concerned has privileged access rights (e.g., domain admin.)

User accounts should be initially suspended or disabled only and not deleted. User account names should not be reused as this may cause confusion in the event of a later investigation.

2.1. User Access Provisioning

Each user must be allocated access rights and permissions to computer systems and data that are commensurate with the tasks they are expected to perform. In general, this should be role-based (i.e., a user account will be added to a group that has been created with the access permissions required by that job role.)

Group roles should be maintained in line with business requirements and any changes to them should be formally authorized and controlled via the change management process. Ad-hoc additional permissions should not be granted to user accounts outside of the group role; if such permissions are required this should be addressed as a change and formally requested.

2.2. Removal or Adjustment of Access Rights

Where an adjustment of access rights or permissions is required (e.g., due to an individual changing role,) this should be carried out as part of the role change. It should be ensured that access rights no longer required as part of the new role are removed from the user account. In the event that a user is taking on a new role in addition to their existing one (rather than instead of) then a new composite role should be requested via change management. Due consideration of any issues of segregation of duties should be given.

Under no circumstances should administrators be permitted to change their own user accounts or permissions.

2.3. Management of Privileged Access Rights

Privileged access rights such as those associated with administrator-level accounts must be identified for each system or network and tightly controlled. In general, technical users (such as IT support staff) should not make day-to-day use of user accounts with privileged access, rather a separate "admin" user account should be created and used only when the additional privileges are required. These accounts should be specific to an individual (e.g., "John Smith Admin"); generic admin accounts should not be used as they provide insufficient identification of the user.

Access to admin level permissions should only be allocated to individuals whose roles require them and who have received sufficient training to understand the implications of their use.
The use of user accounts with privileged access in automated routines such as batch or interface jobs should be avoided where possible. Where this is unavoidable the password used should be protected and changed on a regular basis.

2.4. User Authentication for External Connections

Where remote access to the corporate network is required via VPN, a request must be made via IT Services. Based on assessment of the risk associated with external access, a policy of using two factor authentication for remote access may be required; where required, this access mechanism should conform to the authentication factors of "something you have and something you know" in order to reduce the risk of unauthorized access from the Internet.

Partner agencies or 3rd party suppliers must not be given details of how to access the organization's corporate network without permission. Any changes to supplier's connections (e.g., on termination of a contract) must be immediately sent to the IT Services so that access can be updated or ceased. All permissions and access methods must be controlled by the IT Services.

Partners or 3rd party suppliers must contact the IT Services on each occasion to request permission to connect to the network and a log of activity must be maintained. Remote access software and user accounts must be disabled when not in use.

2.5. Review of User Access Rights

On a regular basis (quarterly) asset and system owners will be required to review who has access to their areas of responsibility and the level of access in place. This will be to identify:

- People who should not have access (e.g., leavers)
- User accounts with more access than required by the role
- User accounts with incorrect role allocations
- User accounts that do not provide adequate identification e.g., generic or shared accounts
- Any other issues that do not comply with this policy

This review will be performed, and any corrective actions identified and carried out.

A review of user accounts with privileged access will be carried out by X on quarterly basis to ensure that this policy is being complied with.

2.6. User Authentication and Password Policy

fpPathfinder's policy is to make use of additional authentication methods (i.e., multi-factor authentication) based on a risk assessment which takes into account:

- The value of the assets protected
- The degree of threat believed to exist
- The cost of the additional authentication method(s)
- The ease of use and practicality of the proposed method(s)
- Any other relevant controls in place

Whether single or multi-factor authentication is used, the quality of user passwords should be enforced in all networks and systems using the following parameters:

Parameter	Value
Minimum length	10
Maximum length	16
Re-use cycle	Cannot be the same as any of the previous 32 passwords
Characters Required	At least one capital letter At least one symbol At least one number
Password similarity	New password cannot share more than three characters in the same position as the old password
Change Frequency	At least every 90 days
Account lockout	On 5 incorrect logon attempts
Account lockout action	Account must be re-enabled by IT Services
Other controls	Password cannot contain the username

Any exceptions to these rules must be authorized by the Information Security Officer.

3. User Responsibilities

Every user has a role to play in ensuring the security of fpPathfinder information. It is vital that every user plays his or her part in protecting the access they have been granted and ensuring that their account is not used to harm the organization. In order to maximize the security of our information every user must:

- Use a strong password in line with the rules set out in this policy
- Never tell anyone their password or allow anyone else to use their account
- Not record the password in writing or electronically (e.g., in a file or email)
- Avoid using the same password for other user accounts, either personal or business-related
- Ensure that any PC or device they leave unattended is locked or logged out
- Leave nothing on display that may contain access information such as login names and passwords
- Inform the IT Services of any changes to their role and access requirements

Failure to comply with these requirements may result in the organization taking disciplinary action against the individual(s) concerned.

4. System and Application Access Control

As part of the evaluation process for new or significantly changed systems, requirements for effective access control should be addressed and appropriate measures implemented.

These should consist of a comprehensive security model that includes support for the following:

- Creation of individual user accounts
- Definition of roles or groups to which user accounts can be assigned
- Allocation of permissions to objects (e.g., files, programs, menus) of different types (e.g., read, write, delete, execute) to subjects (user accounts and groups)
- Provision of varying views of menu options and data according to the user account and its permission levels
- User account administration, including ability to disable and delete accounts
- User logon controls such as
    - Non-display of password as it is entered
    - Account lockout once number of incorrect logon attempts exceeds a specified threshold
    - Provide information about number of unsuccessful logon attempts and last successful logon once user has successfully logged on
    - Date and time-based logon restrictions
    - Device and location logon restrictions
- User inactivity timeout
- Password management, including
    - Ability for user to change password
    - Controls over acceptable passwords
    - Password expiry
    - Hashed/encrypted password storage and transmission
- Security auditing facilities, including logon/logoffs, unsuccessful logon attempts, object access and account administration activities

Access to utility programs that provide a method of bypassing system security (e.g., data manipulation tools) should be strictly controlled and their use restricted to identified individuals and specific circumstances (e.g., as part of a named project or change.)

5. Exceptions

This policy applies to all employees and contractors. Those found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment. This policy does not cover fpPathfinder Platform users as they are provisioned and maintained using tools that are part of that service.

6. Responsibilities

It is the responsibility of all contractors, employees, and management to ensure that this policy is followed.

Third Party Security Requirements Policy

1. Overview

From time to time, fpPathfinder may engage third parties to perform services on behalf of the organization. Such services include but are not limited to:

- Software development support
- Subject matter consultants or professional services
- External equipment or software providers
- Cloud services providers
- Business consultants such as accounting, legal services, or marketing/sales support
- Printing services

It is the position of fpPathfinder that these third parties be disallowed (technically and as a matter of policy) from storing, processing, transmitting, or otherwise accessing confidential and/or customer information. This document outlines the provisions governing such relationships, including requirements for access in the event that business needs dictate such access occur.

2. General Provisions

It is the policy of fpPathfinder in general that third parties are not allowed to access, for any purpose, confidential or customer information. Note that this includes indirect access such as write or administrative access to environments without logical segmentation (e.g., network segmentation) from data storage locations.

To the extent practicable, fpPathfinder has implemented technical controls to enforce this restriction. However, it is a reality that situations may arise where a third party will require access to confidential information to satisfy a legitimate business requirement.

In the event that third party access to this data is required, the following are required:

1. Executive team approval
2. Signed contract, including any information security terms and conditions
3. Documented risk analysis

The following subsections describe each of these requirements in more detail.

3. Executive Team Approval

Documentation of approval by an executive team member will be obtained prior to allowing any third party access to confidential and/or customer information.

4. Information Security Terms and Conditions

Any relationship with a third party that includes access to confidential and/or customer information will be governed contractually, including information security requirements. Such terms and conditions will include, as appropriate:

- Access control
- Asset management
- Communications security
- Compliance
- Cryptography
- Human resources security
- Information security aspects of business continuity management
- Information security incident management
- Information security policies
- Operations security

- Organization of information security
- Physical and environmental security
- Security Policy
- Supplier relationships
- System acquisition, development and maintenance

These agreements will be approved by fpPathfinder management and internal or external counsel as appropriate.

5. Exceptions

This policy applies to all employees and contractors. Those found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

6. Responsibilities

It is the responsibility of all contractors, employees, and management to ensure that this policy is followed.

Software Development Policy

1. Overview

The purpose of this document is to set out fpPathfinder's policy in the development of software applications and components in a way which maximizes their inherent security.

This document sets out the precautions that must be taken during the software development lifecycle to minimize the risk to the organization whilst ensuring that the benefits set out in the original business case for the software are still realized.

As such, this document will represent an initial design for the enhancement of existing development processes and will be updated on at least an annual basis thereafter as fpPathfinder and its needs develop.

2. Software Development Approaches

The process of software development fits in with the higher-level process of project management of new or enhanced information systems.

This process has the following major stages in a project:

- Proposal
- Planning
- Design and Development
- Launch
- Project Closure

The software development lifecycle consists of the following sub-stages:

- Design and Development
- Business requirements specification
- System design
- Development
- Testing

The way in which the stages of the software development lifecycle are approached will depend upon the development approach used. The choice of approach will be made on a project-by-project basis.

3. Security in the Software Development Lifecycle

This section describes the way in which information security considerations should be incorporated into the various stages within the software development lifecycle.

3.1. Business Requirements Specification

The focus within the business requirements stage is on the functionality of the new system. This will be expressed in business rather than technical terms and should tie in with the business case that was produced prior to the initiation of the project.

The business is uniquely placed to give a clear understanding to the development team of the security requirements of the information that the new system will hold and process. In particular the business requirements should specify:

- The value of the information involved
- The sensitivity of the information – will personal data be held?
- Who the information owner is or will be?
- The classification of the information according to the scheme used within the organization

- The environment in which the information will be accessed or processed – will access be available in public areas?
- The criticality of the new system and the information it holds – what is the business impact if it is not available?
- The legal, regulatory and contractual environment the system must operate within

A risk assessment should be carried out as part of the project to ensure that the implications of the above issues are fully understood by all parties.

3.2. System Design

Based on the risk assessment and the classification of the information that is to be held in and processed by the new system, the design must provide for appropriate security features to be available. These will be largely defined by fpPathfinder's established security architecture.

This extends not only to the creation and maintenance of user accounts and permissions but also the following areas:

- Data input validation controls
- Data flow
- Data output
- Interfaces with other systems
- Reporting
- Restart and recovery
- Timestamps
- Logging (e.g., of transactions and access)
- Batch and transaction counters
- Monitoring facilities
- How non-repudiation requirements will be met
- Ongoing patching arrangements
- Use of cryptography
- Need for digital certificates and signatures

These aspects will be included as part of the design documentation when appropriate. The development team will ensure that these areas are considered during each iteration or release and that changes do not invalidate controls implemented during an earlier iteration.

3.3. Development

Before starting to write code, a secure development environment should be established for the project. Depending on the coding environment, languages, databases, tools and other components selected, the appropriate guidelines for secure coding and configuration should be adopted. These should be evaluated to ensure they will provide adequate protection from the various types of potential attack identified in the risk assessment, such as:

- Inputs and buffer overflow
- Time of Check/Time of Use
- Malformed input
- SQL injection

For a lengthy project it will be necessary to obtain regular updates regarding newly identified vulnerabilities and exploits associated with the technology components in use.

3.4. Testing

During the lifecycle of a software application, many different forms of testing will be carried out. Note that the specific testing requirements may vary according to the type of application being developed and the business and security requirements associated with that application. Testing phases may include, but are not limited to unit, system, integration, performance, user acceptance and operational acceptance testing. Security controls will be tested as part of these exercises in a manner commensurate with the sensitivity, criticality, and role of the application. It is recommended that a separate exercise of security testing be carried out against the security requirements that were established during the business requirements and design stages.

Initial security testing should be carried out within the development project with the same degree of rigor and formality as other forms with a suitable range of test inputs being specified.

Once testing has been completed to the development team's satisfaction, a further phase of security testing should be carried out to verify correct operation of controls. The extent of this testing should be in a manner commensurate with the severity and criticality of the application, as well as the extent of the changes made during development activities.

Adequate controls should be put in place to protect test data. Where appropriate (and with prior approval on each occasion), a live to test copy may be made in order to provide representative test data. However, if this contains sensitive information such as personally identifiable data this should be removed or obscured before use.

4. Security in Outsourced Development

Where software development is wholly or partially outsourced to a third party, due care must be taken to ensure that the policies of fpPathfinder are still followed where possible.

4.1. Selection of Outsourced Developer

Standard procurement procedures should be used in the selection and engagement of an appropriate outsourced developer. Use of these procedures should ensure the developer:

- Is capable of delivering the software to the required standard
- Can meet the delivery timescales required
- Represents best value for the organization
- Can meet the security requirements specified

Use of sub-contractors by the outsourced developer for any aspects of the development should be understood and an assessment of these sub-contractors included.

4.2. Communication of Requirements

The contract with the outsourced developer should require compliance with this policy and include a clear statement of the requirements for secure design, coding and testing of the software. The developer should also be required to establish a secure development environment in accordance with fpPathfinder standards.

Requirements definition should be carried out by fpPathfinder so that a clear definition of the software to be created (including its security features) is agreed with the business and used as a contractual starting point for development. While the outsourced developer may in some circumstances assist in the definition of requirements, the exercise should be led, managed and ideally carried out by internal resources so that there is a clear separation between requirements and design/development.

A comprehensive picture of the anticipated threat model faced by the software should be provided to the outsourced developer so that a clear understanding is gained of the types of vulnerabilities that must be avoided if the software is to be secure.

4.3. Supervision and Monitoring

Measures should be put in place to ensure adequate supervision of the activities of the outsourced developer and regular monitoring of progress.

For a large project with significant time gaps between deliverables, an agreed method of verifying interim progress should be in place so that early warning is given of delays.

4.4. Reviews and Acceptance

Review points should be established as part of the project planning process to verify progress and give formal acceptance of the software deliverables created. These will involve appropriate testing activities and code reviews.

The outsourced software developer should be required to provide evidence of the security testing activities carried out during the development, including tests for concealed malware, backdoors and known vulnerabilities.

Where appropriate a security review of developed code may be engaged with a suitable third party with the relevant security expertise.

4.5. Audit of Development Methods

fpPathfinder should have the contractual right to undertake a second party audit of the outsourced development provider. This may be to review whether the development methods used comply with our policies and that all information provided to the supplier is protected by appropriate security controls.

For larger projects it is recommended that an audit be carried out prior to the placing of the order for software development to ensure that assurances given during the sales process are valid.

4.6. Intellectual Property

Unless the software is licensed under a formal agreement, contractual arrangements with an outsourced software developer should state that the ownership of the code produced on our behalf rests with fpPathfinder.

It is important that any software that is developed under an outsourcing contract is understood to be our intellectual property. Appropriate legal advice should be taken particularly if the outsourcer is based outside of our home country.

4.7. Escrow

Arrangements should be made for fpPathfinder to be able to legally access the source code of any developments undertaken in the event that the outsourcer ceases operations. This should be the case during development and if appropriate after the code has been delivered.

5. Exceptions

This policy applies to all employees and contractors. Those found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

6. Responsibilities

It is the responsibility of all contractors, employees, and management to ensure that this policy is followed.

Stacia Waren

Network Services Policy

1. Introduction

This document describes a required minimal security configuration for all networks connecting to a production network or used in a production capacity at or on behalf of fpPathfinder.

2. General Provisions

It is fpPathfinder policy that storage, processing, and transmission of confidential and/or customer data be limited to a discrete, highly-targeted production environment such as that set aside for this purpose in the cloud environment. In the event that data is stored in an on-premise network environment, this document describes the minimum baseline network configuration required to accomplish that safely.

3. Network Segmentation

All environments containing confidential and/or customer data must be logically segmented from networks hosting internal (i.e., employee) communications.

4. Production Routers and Switches

Production routers and switches must meet the following configuration standards:

1. No local user accounts are configured on the router. Routers and switches must use TACACS+ or similar for all user authentication.
2. Passwords on routers or switches must be kept in a secure encrypted form.
3. Access control lists for transiting the device are to be added as business needs arise.
4. Each router must present a login banner prohibiting unauthorized access
5. Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH is the preferred protocol.
6. Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.
7. The corporate router configuration standard will define the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including:
   a. IP access list accounting
   b. Device logging
   c. Incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped
   d. Router console and modem access must be restricted by additional security controls

5. Wireless

All wireless infrastructure devices must:

1. Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol.
2. Use WPA2 Temporal Key Integrity Protocol (TKIP) and/or WPA2 Advanced Encryption System (AES) protocols with a minimum key length of 128 bits.
3. All Bluetooth devices must use Secure Simple Pairing with encryption enabled.
4. Lab device Service Set Identifier (SSID) must be different from production SSIDs.

Home Wireless Requirements:
All home wireless infrastructure devices when used for direct access (e.g., over VPN) to production services, those networks must:

- Enable at least WiFi Protected Access Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS
- Require a complex shared secret key (at least 20 characters) on the wireless client and the wireless access point

- Change the default SSID name
- Change the default login and password

6. Exceptions

This policy applies to all employees and contractors. Those found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

7. Responsibilities

It is the responsibility of all contractors, employees, and management to ensure that this policy is followed.

Change Management Policy

1. Introduction

fpPathfinder provides reliable technology services to customers, employees, contractors and business partners. To do this, changes must be carefully managed to prevent unwanted disruption resulting from a change. The objective of this process is to ensure that changes to IT services and their associated components are recorded and then evaluated, authorized, prioritized, planned, tested, implemented, documented and reviewed in a controlled manner.

2. General Provisions

A change request must be assessed for impact (including information security implications) and resource requirements before being considered. To assist with impact assessment, the identification of related systems/components affected by the proposed change and also input from other affected support groups may be required. After assessment, if the change is deemed acceptable it will be authorized. Once implemented the change will be reviewed and subject to the findings of the review, closed.

Categories of Change:

The following categories of change are used throughout this document:

- Standard
- Normal
- Emergency
- Major

Standard Changes

Standard changes are low-risk, pre-approved changes and so do not need to follow the full review and approval process. Standard changes will be recorded and the implementation process will be fully documented.

Normal Changes

These are “business as usual” changes which are expected to make up the majority of the change requests that are logged and handled through the change management process as described in this document. Although not emergencies, they will be prioritized in order that resources can be allocated in as effective a manner as possible.

Emergency Changes

There will be occasions when business requirements demand that changes be made in an emergency situation. Such changes are those requests which impact on internal or external ‘live’ systems and require implementation to resolve (or prevent) a current high priority incident or problem. In such cases, a change request must be raised immediately even if the full change details are not available.

If an emergency change cannot be formally authorized after reasonable efforts have been made to follow the process (e.g., out of hours) a local decision may be made as to whether this change will be implemented. Details of the change must be recorded, and the change management process followed retroactively to ensure that records are maintained.

Where time allows, the change manager, in collaboration with the relevant support groups, will ensure the following:

- Sufficient staff and resources are available to action and support the change request
- Back-out plans have been documented and passed to the change implementer
- As much testing as possible of the emergency change has been completed
-

Major Changes

Major changes will be logged within the change management process but referred to senior or IT management as their scope and implications will generally encompass a wider audience. They will then be raised as projects with their own business case, project team and budget.

3. Team Roles

The following subsections describe the team members and roles required for the change management process to function. Note that these roles may not necessarily be full time positions or even, in all cases, the same individual each time.

Change Initiator

- May be any stakeholder (employee, contractor, customer) requiring a change in support of a business goal
- Responsible for identifying the need for a change and providing the required information to allow the change request to be assessed
- Works with other team members to scope and document the exact requirements of the change
- May be involved in user acceptance testing of the change once built

Change Manager

- Responsible for identifying improvements to the process and ensuring it is adequately resourced
- Provides information regarding the success rates of the process
- Performs the initial check and classification of changes
- Maintains the change schedule and ensures that all changes are in the correct status

Change Implementer

- Works with the change initiator to define the requirements in more detail
- Creates the items necessary for the change (e.g., new or revised software programs)
- Performs system testing and liaises with the change originator to perform acceptance testing
- Plans the details of the change, tests it prior and post implementation
- Provides feedback to the change manager on the status of the change

Executive Leadership

- Responsible for approving changes

4. Reporting

The Change Manager is responsible for maintaining the change schedule on an ongoing basis. This will set out details of the changes to be implemented. The following information will be included:

- Change description
- Change initiator
- Validation requirements
- Date and time of change
- Possible impacts and workarounds

The following reports, upon request from executive leadership, will be produced by the Change Manager:

- Number of changes raised and closed by week/month
- Breakdown of categories of change requests raised by category (i.e., Normal, Emergency and Major)
- Average time to process a change request of each category
- Percentage successful change requests
- Sources of change requests (e.g., business area)

Requirements for further reports will be reviewed on a regular basis.

5. Exceptions

This policy applies to all employees and contractors. Those found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

6. Responsibilities

It is the responsibility of all contractors, employees, and management to ensure that this policy is followed.

Data Protection Policy

1. Definitions

Company	means fpPathfinder
GDPR	means the General Data Protection Regulation
Responsible Person	means the individual at fpPathfinder responsible for data privacy. Today that is the CEO of fpPathfinder, Michael Lecours
Register of Systems	means a register of all systems or contexts in which personal data is processed by fpPathfinder

2. Data Protection Principles

fpPathfinder has developed its data protection principles to align with article 5 of the GDPR which requires that personal data should be:

a. “processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary for the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organizational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.”

3. General Provisions

a. This policy applies to all personal data processed by fpPathfinder.
b. The Responsible Person shall take responsibility for fpPathfinder’s ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.

4. Lawful, Fair and Transparent Processing

a. To ensure its processing of data is lawful, fair and transparent, fpPathfinder shall maintain a Register of Systems.
b. The Register of Systems shall be reviewed at least annually.
c. Individuals have the right to access their personal data and any such requests made to fpPathfinder shall be dealt with in a timely manner.

5. Lawful Purposes

a. All data processed by fpPathfinder must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).
b. fpPathfinder shall note the appropriate lawful basis in the Register of Systems.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in fpPathfinder's systems.

6. Data Minimization

a. fpPathfinder shall ensure that personal data is adequate, relevant and limited to what is necessary for purposes for which the data is processed.

7. Accuracy

a. fpPathfinder shall take reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

8. Security

a. fpPathfinder shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorized sharing of information.
c. When personal data is deleted, this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.
e. Management will demonstrate commitment to information security by creating and disseminating policy for use throughout the organization
f. Employees will remain cognizant of their security responsibilities and will provide written attestation to security principles

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data, fpPathfinder shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the Client and the Client's employees.

10. Exceptions

This policy applies to all employees and contractors. Those found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

11. Responsibilities

It is the responsibility of all contractors, employees, and management to ensure that this policy is followed.

System Monitoring Policy

1. Introduction

To maintain ongoing compliance with legal, regulatory, and contractual requirements, fpPathfinder will periodically monitor systems. It is fpPathfinder policy that only approved system administrators can access system and network logs. This document describes the procedures employed in gaining access to system and network logs.

2. General Provisions

It is fpPathfinder policy that storage, processing, and transmission of confidential and/or customer data be limited to a discrete, highly-targeted production environment such as that set aside for this purpose in the cloud production environment.

3. Monitoring Requirements

Production cloud environments will employ the security and monitoring capabilities provided by the vendor. In addition, information security may use the following additional capabilities to supplement production monitoring:

- Intrusion Detection/Protection (IDS/IPS)
- Network filtering logs (e.g., firewall, router logs)
- Anti-malware logs
- URL or IP filtering
- Data Loss Prevention (DLP)
- Netflow data

In general, the following should be collected when recording log activity:

- User identification
- Type of event
- Date and time
- Success or failure indication
- Origination of event
- Name of affected data, component, or resource

4. Clock Synchronization

Production cloud environments will employ a secure, reliable time source and ensure that log data is correlated by time.

5. Exceptions

This policy applies to all employees and contractors. Those found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

6. Responsibilities

It is the responsibility of all contractors, employees, and management to ensure that this policy is followed.

Risk Management Policy

1. Introduction

It is the policy of fpPathfinder to ensure that risks that threaten to impact operations, business goals, customer relationships, or have any other detrimental impact to the organization be managed and, to the extent practicable, minimized. Examples of areas covered by this include, but are not limited to:

- Organization-owned data assets such as:
  - business plans
  - financial information
  - employee information
  - organizational records
  - supplier information, relationships and contracts
- Data assets of customers held in trust by fpPathfinder (i.e., customer data)
- Business operations and business practices
- Financial resources including monetary or credit instruments
- Personnel health and safety

To help achieve this, fpPathfinder employs a risk management process to identify risk areas, assess their impact and likelihood, track them over time, and mitigate their impact to an extent commensurate with their value to fpPathfinder or possible negative impact to the organization (or its customers and partners) should the risk come to pass.

2. Objectives

Objectives of this risk management process include:

- Ensure that risk management steps are adopted by all stakeholders to ensure all risk management steps are followed
- To ensure that all employees are aware of the need to assess and mitigate risks in all areas
- To ensure compliance with governing regulation and industry-accepted practices
- The ensure the ability of the organization to carry out its mission in delivering an excellent, reliable, and secure customer experience
- To minimize possible negative outcomes resulting from a risk such as financial or business impacts like fines, loss of market position, or reduced sales

3. General Provisions

This policy applies to all business assets, processes, and data used or processed by fpPathfinder.

4. Risk Management Process

fpPathfinder will employ a multi-stage risk management process consisting of the following phases:

1. Risk identification and assessment
2. Risk treatment
3. Risk monitoring

Each of these phases is outlined in more detail below.

4.1 Risk Identification and Assessment

To minimize risks, the organization must first identify them. Company management will conduct regular risk management meetings, which will include identification and assessment of business, operational, and technical risks. This meeting will occur at least annually or upon significant change to the business, business context, or customer environment. The purpose of this meeting will be to:

- Identify any new, unmanaged and untreated risks that may emerge pursuant to new products or business methods,

- Assess the impact and likelihood of any new risks identified, and
- Update existing risk register documentation to reflect the state of those risks.

Management will conduct (at least annually) a technical risk assessment of the customer environment, reporting all findings to senior management for review during scheduled risk management meetings. In addition, all employees are responsible for reporting newly-identified risks through their management chain as they arise for treatment via this process.

4.2 Risk Monitoring

Management will monitor existing risks to ensure that risks have been treated in a manner commensurate with their impact, and to periodically review risks to ensure they stay within accepted tolerances.

5. Exceptions

This policy applies to all employees and contractors. Those found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

6. Responsibilities

It is the responsibility of all contractors, employees, and management to ensure that this policy is followed.

Information Security Incident Response Procedure

1. Introduction

This document is intended to be used when an incident of some kind has occurred that affects the information security of fpPathfinder. It is intended to ensure a quick, effective and orderly response to information security incidents.

The procedures set out in this document should be used only as guidance when responding to an incident. The exact nature of an incident and its impact cannot be predicted with any degree of certainty and so it is important that a good degree of common sense is used when deciding the actions to take. However, it is intended that the structures set out here will prove useful in allowing the correct actions to be taken more quickly and based on more accurate information.

The objectives of this incident response procedure are to:

- Provide a concise overview of how fpPathfinder will respond to an incident affecting its information security
- Set out who will respond to an incident and their roles and responsibilities
- Describe the facilities that are in place to help with the management of the incident
- Define how decisions will be taken with regard to our response to an incident
- Explain how communication within the organization and with external parties will be handled
- Provide contact details for key people and external agencies
- Define what will happen once the incident is resolved, and the responders are stood down.

All personal information collected as part of the incident response procedure and contained in this document will be used purely for the purposes of information security incident management and is subject to relevant data protection legislation.

2. Incident Response Flowchart

The flow of the incident response procedure is shown in the diagram below.

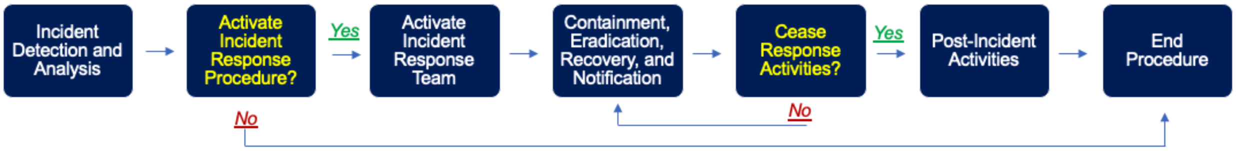

Incident Detection and Analysis
Activate Incident Response Procedure?
Yes
No
Activate Incident Response Team
Containment, Eradication, Recovery, and Notification
Cease Response Activities?
Yes
No
Post-Incident Activities
End Procedure

Figure 1 - Incident response flowchart

These steps are explained in more detail in the rest of this procedure.

3. Incident Detection and Analysis

The incident may be initially detected in a wide variety of ways and through a number of different sources, depending on the nature and location of the incident. Some incidents may be self-detected via software tools used within fpPathfinder or by employees noticing unusual activity. Others may be notified by a third party such as a customer, supplier, or law enforcement agency who has become aware of a breach.

It is not unusual for there to be a delay between the origin of the incident and its actual detection; one of the objectives of this policy is to reduce this time period. The most important factor is that the incident response procedure must be started as quickly as possible after detection so that an effective response can be given.

Once the incident has been detected, an initial impact assessment must be carried out in order to decide the appropriate response. This impact assessment should estimate:

- The extent of the impact on IT infrastructure including computers, networks, equipment, and accommodation
- The information assets that may be at risk or have been compromised
- The likely duration of the incident i.e., when it may have begun
- The business units affected and the extent of the impact to them
- Initial indication of the likely cause of the incident

This information should be documented so that a clear time-based understanding of the situation as it emerges is available for current use and later review.

A list of the information assets, business activities, products, services, teams, and supporting processes that may have been affected by the incident should be created together with an assessment of the extent of the impact.

As a result of this initial analysis, any member of the management team has the authority to contact the Incident Response Team Leader at any time to ask him/her to assess whether the Incident Response Procedure should be activated.

4. Activating the Incident Response Procedure

Once notified of an incident the Team Leader must decide whether the scale and actual or potential impact of the incident justifies the activation of the Incident Response Procedure and the convening of an Incident Response Team (IRT).

Guidelines for whether a formal incident response should be initiated for any particular incident of which the Team Leader has been notified are if any of the following apply:

- There is significant actual or potential loss of classified information
- There is significant actual or potential disruption to business operations
- There is significant risk to business reputation
- Any other situation which may cause significant impact to the organization

In the event of disagreement or uncertainty about whether or not to activate an incident response, the decision of the Team Leader will be final. If it is decided not to activate the procedure, then a plan should be created to allow for a lower level response to the incident within normal management channels. This may involve the invocation of relevant procedures at a local level. If the incident warrants the activation of the IR procedure the Team Leader will start to assemble the IRT.

5. Assemble Incident Response Team

Once the decision has been made to activate the incident response procedure, the Team Leader will ensure that all roles are contacted, made aware of the nature of the incident and asked to assemble at an appropriate location.

The exception is the Incident Liaison who will be asked to attend the location of the incident (if different) in order to start to gather information for the incident assessment that the IRT will conduct so that an appropriate response can be determined.

5.1 Incident Response Team Members

A given Incident Response Team will generally consist of the following roles specified and with the stated deputies, although the exact make-up of the team will vary according to the nature of the incident. For example, an incident response team may require participants representing:

- fpPathfinder executives
- Information technology
- Business operations
- Human resources

- Public relations
- Legal (internal or external counsel)
- Others as appropriate

It is the responsibility of the incident response team leader, or the team facilitator as his/her delegate, to determine the correct makeup and personnel required to support a given incident and to include others as the situation requires.

5.2 Roles and Responsibilities
The responsibilities of the roles within the incident response team are as follows:

Team Leader

- Decides whether or not to initiate a response
- Assembles the incident response team
- Overall management of the incident response team
- Acts as interface with the board and other high-level stakeholders
- Final decision maker in cases of disagreement
- Assesses the extent and impact of the incident
- Provides first-person account of the situation to the IRT
- Provide advice on business continuity options
- Invoke business continuity plans if required

Team Facilitator

- Supports the incident response team
- Co-ordinates resources within the command center
- Prepares for meetings and takes record of actions and decisions
- Briefs team members on latest status on their return to the command center
- Facilitates communication via email, fax, telephone or other methods
- Monitors external information feeds such as news

Information Technology

- Provides input on technology-related issues
- Assists with impact assessment

Business Operations

- Contributes to decision-making based on knowledge of business operations, products and services
- Briefs other members of the team on operational issues
- Helps to assess likely impact on customers of the organization
- Deals with aspects of physical security and access
- Provides security presence if required
- Assesses the incident for any health and safety impacts
- Ensures that legal responsibilities for health and safety are met at all times
- Liaises with emergency services such as police, fire and medical
- Considers environmental issues with respect to the incident

Human Resources

- Assesses and advises on HR policy and employment contract matters
- Represents the interests of organization employees
- Advises on capability and disciplinary issues

Communications/PR

- Responsible for ensuring internal communications are effective

- Decides the level, frequency and content of communications with external parties such as the media
- Defines approach to keeping affected parties informed (e.g., customers, shareholders)

Legal and Regulatory

- Advises on what must be done to ensure compliance with relevant laws and regulatory frameworks
- Assesses the actual and potential legal implications of the incident and subsequent actions

Unless otherwise designated at the time of an incident, the above roles will be held by Michael Lecours and Stacia Waren.

5.3 Incident Management, Monitoring and Communication

Once an appropriate response to the incident has been identified, the IRT needs to be able to manage the overall response, monitor the status of the incident, and ensure effective communication is taking place at all levels.

During an incident, the Incident Liaison will provide updates to the IRT to a frequency decided by the Team Leader. These updates should be coordinated with the IRT meetings so that the latest information is available for each meeting.

5.4 Communication Procedures

It is vital that effective communications are maintained between all parties involved in the incident response.

The primary means of communication during an incident will initially be face to face and telephone, both landline and mobile. Email or other electronic messaging should not be used unless permission to do so has been given by the IRT.

The following guidelines should be followed in all communications:

- Be calm and avoid lengthy conversation
- Advise internal team members of the need to refer information requests to the IRT
- If the call is answered by someone other than the contact:
  - Ask if the contact is available elsewhere
  - If they cannot be contacted leave a message to contact you on a given number
  - Do not provide details of the Incident
- Always document call time details, responses and actions

All communications should be clearly and accurately recorded as records may be needed as part of legal action at a later date.

5.4.1 External Communication

Depending on the incident there may be a variety of external parties that will be communicated with during the course of the response. It is important that the information released to third parties is managed so that it is timely and accurate. Calls that are not from agencies directly involved in the incident response (such as the media) should be passed to the member of the IRT responsible for communications.

There may be a number of external parties who, whilst not directly involved in the incident, may be affected by it and need to be alerted to this fact. These may include:

- Customers
- Suppliers
- Stakeholders
- Regulatory bodies

The Communications IRT member should make a list of such interested parties and define the message that is to be given to them. A list of some external agencies is held by the persons responsible for such communications.

Interested parties who have not been alerted by the IRT may call to obtain information about the incident and its effects. These calls should be recorded in a message log and passed to the Communications member of IRT.

5.4.2 Communication with the Media

In general, the communication strategy with respect to the media will be to issue updates via top management. No members of staff should give an interview with the media unless this is pre-authorized by the IRT.

The preferred interface with the media will be to issue pre-written press releases. In exceptional circumstances a press conference will be held to answer questions about the incident and its effects. It is the responsibility of the Communications IRT member to arrange the venue for these and to liaise with press that may wish to attend.

6. Incident Containment, Eradication, Recovery and Notification

6.1 Containment

The first step will be to try to stop the incident getting any worse (i.e., contain it.) In the case of a malware outbreak, this may entail disconnecting the affected parts of the network. For a hacking attack it may involve disabling certain profiles or ports on the firewall or perhaps even disconnecting the internal network from the Internet altogether. The specific actions to be performed will depend on the circumstances of the incident.

Note: if it is judged to be likely that digital evidence will need to be collected that will later be used in court, precautions must be taken to ensure that such evidence remains admissible. This means that relevant data must not be changed either deliberately or by accident e.g., by waking up a laptop. It is recommended that specialist advice should be obtained at this point.

Particularly (but not exclusively) if foul play is suspected in the incident, accurate records must be kept of the actions taken and the evidence gathered in line with digital forensics guidelines. The main principles of these guidelines are as follows:

Principle 1 – Don’t change any data. If anything is done that results in the data on the relevant system being altered in any way, then this will affect any subsequent court case.

Principle 2 – Only access the original data in exceptional circumstances. A trained specialist will use tools to take a bit copy of any data held in memory, whether it’s on a hard disk, flash memory or a SIM card on a phone. All analysis will then take place on the copy and the original should never be touched unless in exceptional circumstances e.g., time is of the essence and gaining information to prevent a further crime is more important than keeping the evidence admissible.

Principle 3 – Always keep an audit trail of what has been done. Forensic tools will do this automatically, but this also applies to the first people on the scene. Taking photographs and videos is encouraged as long as nothing is touched to do it.

Principle 4 – The person in charge must ensure that the guidelines are followed. Prior to the arrival of a specialist basic information should be collected. This may include:

- Photographs or videos of relevant messages or information
- Manual written records of the chronology of the incident

- Original documents, including records of who found them, where and when
- Details of any witnesses

Once collected, the evidence will be kept in a safe place where it cannot be tampered with and a formal chain of custody established.

The evidence may be required:

- For later analysis as to the cause of the incident
- As forensic evidence for criminal or civil court proceedings
- In support of any compensation negotiations with software or service suppliers

Next, a clear picture of what has happened needs to be established. The extent of the incident and the implications should be ascertained before any kind of containment action can be taken.
Audit logs may be examined to piece together the sequence of events; care should be taken that only secure copies of logs that have not been tampered with are used.

6.2 Eradication

Actions to fix the damage caused by the incident, such as deleting malware, must be put through the change management process (as an emergency change if necessary). These actions should be aimed at fixing the current cause and preventing the incident from re-occurring. Any vulnerabilities that have been exploited as part of the incident should be identified.

Depending on the type of incident, eradication may sometimes be unnecessary.

6.3 Recovery

During the recovery stage, systems should be restored back to their pre-incident condition, although necessary actions should then be performed to address any vulnerabilities that were exploited as part of the incident. This may involve activities such as installing patches, changing passwords, hardening servers and amending procedures.

6.4 Notification

The notification of an information security incident and resulting loss of data is a sensitive issue that must be handled carefully and with full management approval. The IRT will decide, based on legal and other expert advice and as full an understanding of the impact of the incident as possible, what notification is required and the form that it will take.

fpPathfinder will always comply in full with applicable legal and regulatory requirements regarding incident notification and will carefully assess any offerings to be made to parties that may be impacted by the incident, such as credit monitoring services.

Records collected as part of the incident response may be required as part of any resulting investigations by relevant regulatory bodies and fpPathfinder will cooperate in full with such proceedings.

Post-Incident Activity

The Team Leader will decide, based on the latest information from the Incident Liaison and other members of the team, the point at which response activities should be ceased and the IRT stood down. Note that the recovery and execution of plans may continue beyond this point but under less formal management control.

This decision will be up to the Team Leader's judgment but should be based upon the following criteria:

- The situation has been fully resolved or is reasonably stable
- The pace of change of the situation has slowed to a point where few decisions are required
- The appropriate response is well underway and recovery plans are progressing to schedule

- The degree of risk to the business has lessened to an acceptable point
- Immediate legal and regulatory responsibilities have been fulfilled

If recovery from the incident is on-going the Team Leader should define the next actions to be taken. These may include:

- Less frequent meetings of the IRT (e.g., weekly depending on the circumstances)
- Informing all involved parties that the IRT is standing down
- Ensuring that all documentation of the incident is secured
- Requesting that all staff not involved in further work to return to normal duties
- All actions taken as part of standing down should be recorded

After the IRT has been stood down the Team Leader will hold a debrief of all members ideally within 24 hours. The relevant records of the incident will be examined by the IRT to ensure that they reflect actual events and represent a complete and accurate record of the incident. Any immediate comments or feedback from the team will be recorded.

A more formal post-incident review will be held at a time to be decided by top management according to the magnitude and nature of the incident.

7. Exceptions

This policy applies to all employees and contractors. Those found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

8. Responsibilities

It is the responsibility of all contractors, employees, and management to ensure that this policy is followed.

Employee Disciplinary Process

1. Introduction

Our Disciplinary Action policy explains how we address employees' misconduct or inadequate performance. Employees must be aware of the consequences of their actions. This policy applies to all our employees.

2. Policy Elements

The stages that may be followed when discipline is deemed necessary include the following:

1. Verbal warning
2. Corrective Actions/Counseling
3. Official written reprimand
4. Disciplinary meeting with appropriate supervisor or manager
5. Final written warning
6. Detraction of benefits
7. Indefinite suspension or demotion
8. Termination

2.1 The nature of the offense must be explained to the employee from the beginning of the procedure. The verbal warning may take the form of a simple oral reprimand but also a full discussion if that is necessary.

The employee must read and sign the written reprimand and final written warning. These documents include the time limit in which an employee must correct their conduct before we take further disciplinary action.

2.2 The following scenarios indicate where the disciplinary procedure starts depending on the violation:

Performance issues. Disciplinary procedure starts at stage 1. It includes but is not limited to:

- Failure to meet performance objectives.
- Attendance issues.
- Failure to meet deadlines.

Misdemeanors/One-time minor offense. Disciplinary procedure starts at stage 1. It includes but is not limited to:

- Rude behavior to co-workers, customers, or partners.
- On-the-job minor mistakes.
- Breach of dress code/open door policy etc.
- Involuntary Discrimination.

Misconduct/Frequent offender. Disciplinary procedure starts at stage 5. It includes but is not limited to:

- Lack of response to counseling and corrective actions.
- Lost temper in front of customers or partners.
- On-the-job major mistakes.
- Unwillingness to follow health and safety standards.

Severe offensive behavior/Felony. Disciplinary procedure starts at stage 6. It includes but is not limited to:

- Corruption/ Bribery.
- Breach of employment agreement.
- Harassment/ Voluntary discrimination.
- Workplace Violence.
- Embezzlement/Fraud.

- Substance Abuse.

Managers or HR may choose to repeat stages of our disciplinary procedure as appropriate.

2.3 Our disciplinary procedure begins when there is sufficient evidence to justify it. When there is suspicion or hints of misconduct, managers or HR must investigate the matter first.

2.4 Appeals are allowed and must be filed to the next line of management as soon as possible.

2.5 HR and managers should document every stage of our disciplinary procedure (except the verbal warning.) If appropriate, include necessary information like evidence, testimonies, and employee's progress or improvement.

2.6 We are obliged to refrain from disciplinary actions that may constitute retaliatory behavior. A no retaliation company policy will be effective at all times to ensure there is no misuse of our disciplinary procedure.

2.7 We have the right to modify this policy or act in any other legal or reasonable way as each case demands. We will always enforce discipline in a fair and lawful manner.

3. Exceptions

This policy applies to all employees and contractors. Those found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

4. Responsibilities

It is the responsibility of all contractors, employees, and management to ensure that this policy is followed.

Clear Desk, Clear Screen Policy

1. Introduction

It is the responsibility of fpPathfinder personnel to ensure that sensitive information is protected when not in use. To ensure that sensitive information is not disclosed to unauthorized parties, employee workspaces should be kept free of written materials containing sensitive information and workstation screens should be locked when not in use to prevent accidental disclosure of information.

2. General Provisions

All confidential materials should be locked away and/or hidden from view when not in use. Likewise, employee workstations should be locked when not in use.

3. Clear Desk, Clear Screen

All work areas should remain free of paper (hardcopy) and/or electronic media unless that information is being actively used. Electronic media and paper records should be stored in locked cabinets at the end of the day. Keys for locked cabinets must be protected such as with the employee and not stored in the same work area as the cabinet.

Computer workstations should be locked when not in use and secured (either locked or powered down) at the end of the workday.

Whiteboards must be scrubbed clean of sensitive information at the conclusion of use. Conference facilities (video sharing, monitors, etc.) should be cleared of sensitive information when not in use.
All media and paper records should be shredded or otherwise securely destroyed when no longer required.

4. Exceptions

This policy applies to all employees and contractors. Those found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

5. Responsibilities

It is the responsibility of all contractors, employees, and management to ensure that this policy is followed.

Acceptable Use Policy

1. Introduction

fpPathfinder may make resources available to employees, contractors, and others to enable to them to optimally perform their duties, or in some cases for their convenience, while on fpPathfinder premises or while performing fpPathfinder work. It is expected that those to whom these services and resources are made available will adhere to the provisions of acceptable use contained within this document.

2. General Provisions

This policy applies to all resources owned, used, or managed by fpPathfinder.

3. Acceptable use of assets

3.1 Ownership of Technology Resources

Computers and mobile devices provided to employees or contractors for work purposes are the property of the organization and may be accessed, monitored, deactivated, or otherwise modified at any time for any reason.

3.2 Consent to Monitoring

To ensure robust security and compliance with applicable legal, regulatory, and contractual obligations, fpPathfinder may routinely monitor activity on networks, log and review actions taken on company-issued devices, and otherwise passively and actively monitor technology use. By using these resources, employees consent to such monitoring.

3.3 Prohibited Activities

fpPathfinder is a professional, safe, and harassment-free workplace. Behavior that runs contrary to these principles is explicitly prohibited while on fpPathfinder premises or while employees act as a representative of fpPathfinder in public forums. Additionally, use of fpPathfinder resources (including but not limited to Internet access) for unprofessional, violent, harassing, or other activities is prohibited. This includes but is not limited to:

- Creating, downloading, uploading, displaying or knowingly accessing sites that contain pornography or other “unsuitable” material that might be deemed illegal, obscene or offensive
- Sharing of copyrighted music, video or image files
- Online gambling
- Running a personal business
- Downloading or running “pirate” software (i.e., use of software in violation of its licensing terms)
- Sending harassing or threatening messages via email, public forum, or through direct message
- Stalking or profiling others without their consent
- Creating, posting, or forwarding “hate speech” such as racial slurs or derogatory statements
- Fraud or “hacking”

Employees or contractors engaging in this behavior are subject to disciplinary action, including termination.

3.4 Right to Censor

To help enforce a professional workplace, the organization may block certain websites or categories of websites. These may include, but are not limited to, those containing illegal materials, that promote illegal activity, pornography, that promote violence or hate speech, or any other material that fpPathfinder determines is inappropriate for the workplace.

4. Exceptions

In some situations, employees may have a need to access sites in support of approved business purposes that would otherwise be in violation of this policy. Individual cases will be reviewed with the employee’s manager, who is responsible for making a determination, and providing documented approval.

5. Responsibilities

It is the responsibility of all contractors, employees, and management to ensure that this policy is followed.

Employee Screening Policy

1. Introduction

fpPathfinder customers may include those with regulatory and contractual requirements that preclude high risk individuals (e.g., those convicted of fraud, those without authorization to work within the United States, etc.) from accessing their systems and data. As fpPathfinder Personnel may periodically, in the course of their duties, come in contact with such data, it is the policy of the firm that background checks will be conducted on all employees and contractors.

2. General Provisions

Employment at fpPathfinder is contingent upon the results of a background check. Background checks will be conducted within 30 days after employment begins and may be conducted periodically afterward.

3. Background Check Requirements

In general, background checks will include but are not necessarily limited to:

- Verification of US citizenship and/or work authorization
  - Social security number and/or work authorization number
  - Date of birth
  - Aliases or alternate names used in official and/or legal correspondence
  - Any current and former residential addresses
- Professional qualifications
  - Verification of employment history
  - Verification of education
- References
  - Professional references
  - Personal references (if applicable)
- Criminal history

Some jobs will, of necessity or to comply with applicable law, require enhanced screening. Subject to the requirements of the individual position, background checks may also extend to:

- Driver history and/or motor vehicle records
- Credit history (excepting bankruptcy status)

4. Exceptions

It is contrary to US law (specifically the Fair Credit Reporting Act) to consider bankruptcy status as a condition of employment. As such, in the event a credit history is called for, bankruptcy status will not be considered.

5. Responsibilities

It is the responsibility of all contractors, employees, and management to ensure that this policy is followed.

Malicious Code Policy

1. Introduction

The purpose of this policy is to reduce the risk of malware, ransomware, worms, trojans, viruses, and any other malicious code impacting fpPathfinder business activities.

2. General Provisions

This policy applies to all computers, laptops, PC, or other computing devices used by fpPathfinder employees.

3. Malicious Code

To reduce impact to customers and business operations, fpPathfinder will employ technical controls to safeguard against the transmission of malware and/or malicious code.

3.1 Protection Measures for Internal Business Environment

Where feasible, fpPathfinder will employ malicious code protection mechanisms at all network ingress and egress points, including email filtering. All desktops and laptops will employ endpoint protection software (e.g., anti-virus scanners) to detect and remove malicious code. These mechanisms will be kept current and signatures will be updated on a regular basis (e.g., daily or weekly).

3.2 Protection Measures for Customer Data Environments

It is of particular importance that customer environments remain malware free. In addition to the above requirements, customer environments will remain segmented at the network level from internal environments (e.g., the internal network environment), using additional network ingress and egress filtering to minimize the likelihood of malware transmission. All customer environments must employ backup measures to ensure the timely restoration of data pursuant to fpPathfinder backup and restoration policies. Where feasible, customer environments must use anti-exploitation technologies (DEP, ASLR, fstack protection, or other) to minimize malware transmission.

3.3 Employee Training

In addition to technical countermeasures, fpPathfinder will conduct training and awareness activities geared to employees about malware, phishing, and other security topics. This may include (but is not necessarily limited to) computer-based training, in-person training, phishing or attack simulation, and other techniques. It is the responsibility of all employees to employ discretion and vigilance in opening links or attachments received through email, to alert IT of possible malware or suspicious emails, and to inform management promptly in the event of accidental malware infection.

4. Exceptions

Some platforms may be incapable of running malware scanning software. Likewise, some platforms (such as mobile phones, Linux, etc.) may be somewhat less “at risk” for malware than others due to the relative prevalence of malware written for those platforms relative to others. fpPathfinder management may review, on a case by case basis situations where malware prevention technology is unavailable and select alternate, compensating controls instead.

5. Responsibilities

It is the responsibility of all contractors, employees, and management to ensure that this policy is followed.

Data Classification Policy

1. Introduction

fpPathfinder data and data held in trust by fpPathfinder on behalf of customers must be protected according to its value. Accomplishing this requires that personnel know and understand the sensitivity of data in order to do so. This policy defines how data is to be classified and labeled within the firm.

2. General Provisions

This policy applies to all data used or processed by fpPathfinder.

3. Data Classification

3.1 Classification System

fpPathfinder uses a classification system that groups information according to sensitivity:

- **Public information** – Information that is approved for external (public) release; no confidentiality protection is required for this information although this information must be protected against unauthorized tampering.
- **Internal Use** – Information that is approved for internal distribution or for distribution to external parties to support business goals; employees and approved contractors must take steps to prevent this information from being made available to unauthorized parties.
- **Confidential** – Information that may expose the firm to potential financial penalties or legal liabilities. Access may be granted based on need to know in accordance with all organizational policy.
- **Customer Information** – Any customer information.

3.2 Data Labeling

Where possible, information assets must be labeled according to the value of the data they store. Where not possible to label assets, information may be logically grouped in such a way that label is implicit: for example, data within a customer cloud environment may be considered “Confidential” while data within corporate email systems (which are precluded from storing, processing, or transmitting customer information) may be labeled “Internal Use”.

4. Exceptions

There are no exceptions to this policy. Situations can arise where technology prevents individual data items, records or documents from being protected fully in accordance with its classification level. These will be reviewed and the associated risks documented in accordance with risk management objectives and governing policy.

5. Responsibilities

It is the responsibility of all contractors, employees, and management to ensure that this policy is followed.

Termination Policy

1. Introduction

fpPathfinder Termination/Separation of Employment policy refers to the event that an employee ceases to be part of fpPathfinder workforce. It is beneficial for all parties that the employment separation process is as clear as possible so misunderstandings and distrust between the employee and fpPathfinder can be avoided. fpPathfinder is bound to handle any cases of termination of employment as dictated by law with discretion, professionalism and official documentation.

2. General Provisions

fpPathfinder will observe all legal dictations referring to termination/separation of employment and will avoid "implied contracts" and unnecessary terminations.

What is termination of employment?

Termination of employment happens when the contract of an employee is discontinued due to their or fpPathfinder's actions. The dismissal of an employee from their job duties may be categorized as voluntary or involuntary.

Voluntary dismissal may include the following:

- Resignation
- Retirement
- Failure to show for a specified number of days without notice
- Expiration or completion of contract

Involuntary dismissal may include the following:

- Discharge for cause
- Discharge without cause

Discharge for cause refers to immediate termination of employment due to an employee's misconduct. Any kind of disciplinary action or progressive discipline that results in termination may be considered "for cause". Other wrongful behaviors or actions that result in immediate dismissal are also considered "for cause". Examples of such termination of employees include circumstances where an employee:

- Breaches their contract of employment
- Is discovered guilty of fraud, embezzlement or other kinds of illegal actions against fpPathfinder
- Is guilty of discriminatory behavior or harassment
- Is guilty of unlawful or immoral behavior on the job
- Is guilty of willful neglect of job responsibilities
- Is discovered to have caused intentional damage to company's assets
- Continuously disregards company policy

The list is not exhaustive therefore, discharge for cause remains at fpPathfinder discretion. It must however always reflect an unacceptable behavior or action that violates legal or company guidelines and may result in financial and non-financial damages for fpPathfinder, other employees or society.

Discharge without cause can occur when fpPathfinder decides that the services of an employee are no longer needed. In general, this does not refer to an employee's conduct. Reasons for discharge without cause may be layoffs, rearrangement of a department or redefining of a position. In cases an employee must be terminated without cause, fpPathfinder is obliged to give notice a specified amount of time prior to the date of termination depending on time of service, age of employee or position. If the employee has to stop working before the date of termination, fpPathfinder will still provide compensation for the time remaining, specified as "pay in lieu of notice".

fpPathfinder may compensate the terminated employee for accrued vacation time when appropriate. Severance pay may apply to cases of discharge without cause but not discharge for cause. fpPathfinder is bound by the law to refrain from wrongful dismissals of employees. Wrongful dismissal may occur in cases when:

- An employee is terminated unfairly for cause
- An employee is terminated without cause and is not given prior notice
- An employee is forced into constructive dismissal

fpPathfinder expects all employees with the right of terminating subordinates to strictly refrain from discharging someone without adequate reason or without giving notice. Such an occurrence may be damaging for fpPathfinder's respectability and may result in disciplinary action. Discharge on grounds of discrimination or filed health and safety complaints is unlawful termination prohibited by legislation.

Constructive dismissal refers to an employee that has been forced to resign due to an employer's intentional or unintentional unlawful or hostile behavior (e.g., breach of contract). It will not be practiced by any means by fpPathfinder which is committed to maintain a relationship of honesty and fairness between itself and employees.

3. Procedure

In cases of resignation, the employee must submit an official written resignation letter to their immediate supervisor. A notice is expected by the employee consistent with the minimum notice requirement, so fpPathfinder can arrange alternatives for handling the remaining workload of the position. The resignation letter must be copied and submitted to the Human Resources department.

In cases of involuntary dismissal, the supervisor must submit written notification to the human resources department at the date of separation or before that. Discharge for cause justifies immediate suspension until the necessary documentation for termination has been gathered. In some instances, a termination meeting with the employee, supervisor and a human resources officer may be scheduled.

In cases of discharge without cause, the employer must officially notify the employee of the termination a specified amount of time in advance. When severance pay is appropriate it will be officially stated in writing. At all times, proper employee records will be kept containing all relevant documentation. Legal counsel may be consulted prior to termination so fpPathfinder can ensure the legality of its actions.

All company owned assets must be returned to fpPathfinder and user access must be terminated per the access control policy.

4. Exceptions

This policy applies to all employees and contractors. Those found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

5. Responsibilities

It is the responsibility of all contractors, employees, and management to ensure that this policy is followed.

Mobile Device Policy

1. Overview

Mobile devices, such as smartphones and tablet computers, are important tools for the organization and fpPathfinder supports their use to achieve business goals. However, mobile devices also represent a significant risk to data security as, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorized access to the organization's data and IT infrastructure. This can subsequently lead to data leakage and system infection.

fpPathfinder has a requirement to protect its information assets to safeguard its customers, intellectual property, and reputation. This document outlines a set of practices and requirements for the safe use of mobile devices and applications.

2. General Provisions

All mobile devices, whether owned by fpPathfinder or owned by employees, inclusive of smartphones and tablet computers, that have access to corporate networks, data and systems are governed by this mobile device security policy. The scope of this policy does not include corporate IT-managed laptops. Applications used by employees on their own personal devices which store or access corporate data, such as cloud storage applications, are also subject to this policy.

3. Mobile Device Requirements

Technical Requirements

Devices must use the following Operating Systems: the most recent versions are recommended, where not possible the operating systems must be still under support for security patches by the manufacturer. Devices must be configured with a secure password that complies with fpPathfinder's password policy. This password must not be the same as any other credentials used within the organization. Devices must employ a screen lock and allow "remote wiping" in the event the device is lost or stolen. Devices must not be "jailbroken" or "rooted" or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user. Devices must be kept up to date with manufacturer or network provided patches.

4. Usage Requirements

Users may only load corporate data that is essential to their role onto their mobile device(s). Users must report all lost or stolen devices to fpPathfinder immediately. If a user suspects that unauthorized access to company data has taken place via a mobile device, they must report the incident in alignment with fpPathfinder incident handling procedures.

Users must not load pirated software or illegal content onto their devices. Applications must only be installed from official platform-owner approved sources. Installation of software from untrusted sources is forbidden.

The user is responsible for the backup of their own personal data and fpPathfinder will accept no responsibility for the loss of files due to a device being wiped by fpPathfinder for security reasons.

5. Exceptions

This policy applies to all employees and contractors. Those found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

6. Responsibilities

It is the responsibility of all contractors, employees, and management to ensure that this policy is followed.

Evidence Collection and Retention

1. Overview

In the event of a security breach or suspected breach, it may become necessary for fpPathfinder to retain evidence to be used in furtherance of legal action, prosecution, or other proceeding. Therefore, fpPathfinder seeks to ensure that all such evidence is collected in a manner that supports this and that, to the extent required by law, refrains from interference with law enforcement activities.

2. General Provisions

Given fpPathfinder's size, business, culture, and operating model, we do not as a general rule maintain forensic specialists on staff. Therefore, should forensic examination of computer systems, servers, applications, mobile phones, or other electronic equipment be required, fpPathfinder will:

- Defer to law enforcement personnel on the collection and examination of evidence,
- Comply with all commercially reasonable law enforcement requests where possible (in consultation with fpPathfinder legal counsel)
- Comply with valid court orders and legal directives

If a matter requires collection of evidence not in support of law enforcement activities (for example, to offer expert testimony pursuant to a civil proceeding), fpPathfinder will engage a subject matter specialist such as a firm specializing in evidence collection and forensic examination. In such cases, chain of custody of evidence will be preserved throughout the collection and examination of potential evidence.

3. Exceptions

This policy applies to all employees and contractors. Those found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

4. Responsibilities

It is the responsibility of all contractors, employees, and management to ensure that this policy is followed.

Software Installation Policy

1. Introduction

Allowing employees to install software on company computing devices opens the organization up to unnecessary exposure. Conflicting file versions or DLLs which can prevent programs from running, the introduction of malware from infected installation software, unlicensed software which could be discovered during audit, and programs which can be used to hack the organization's network are examples of the problems that can be introduced when employees install software on company equipment.

2. Policy Elements

The purpose of this policy is to outline the requirements around the installation of software on fpPathfinder computing devices to minimize the risk of loss of program functionality, the exposure of sensitive information contained within fpPathfinder's computing network, the risk of introducing malware, and the legal exposure of running unlicensed software. This policy covers all computers, servers, smartphones, tablets and other computing devices operating within fpPathfinder.

- Employees may not install software on fpPathfinder computing devices operated within fpPathfinder network unless it is approved by the executive team.
- Software requests must be made to the executive team via email.
- The executive team will be responsible for obtaining and tracking the licenses, testing new software for conflict and compatibility, and performing the installations.

3. Exceptions

This policy applies to all employees and contractors. Those found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

4. Responsibilities

It is the responsibility of all contractors, employees, and management to ensure that this policy is followed.

Backup Policy

1. Introduction

Data can be destroyed by system malfunction or accidental or intentional means. Adequate backups will allow data to be readily recovered as necessary. The ongoing availability of data is critical to the operation of fpPathfinder. In order to minimize any potential loss or corruption of this data the organization needs to ensure data is adequately backed up by establishing and following an appropriate system backup procedure.

2. Policy Elements

This policy ensures certain controls via technical and organizational measures, both with processing data for one's own purposes and with commissioned data processing; in this context, an availability control applies in particular.

Verification of the controls or technical and organizational measures is to be provided to customers within the scope of commissioned data processing.

3. General Regulations

- Data backup must be performed responsibly and competently
- No accidental bypassing of authorization models by data backup measures
- Confidentiality and obligation to data protection
- Nomination of people responsible for each task area
- Determine need for confidentiality, integrity and availability

4. Technical Implementation

- Determine retention period and number of generations
- Sufficient documentation and logging: especially backup data, backup scope, backup parameters
- Arrange the recovery procedure
- Create inventory directory
- Ensure the evaluation of logs
- Tests on data reconstruction/restoration and emergency drills
- Set up necessary controls, especially access control
- Implement the protection requirements for confidentiality, integrity and availability
- Specify and secure transport routes
- Allocate capacities: throughput, volume, quantity of data-storage devices
- Implement requirements for seamless backup (mobile computers, PDA/MDA, databases, open files, system data, log data, etc.)
- Especially ensure access control, access-permission control, transmission control, input control and separation control, also with regard to data backup sets.

5. Exceptions

This policy applies to all employees. Employees found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

6. Responsibilities

It is the responsibility of all employees and management to ensure that this policy is followed.

Business Continuity and Disaster Recovery Plan (BCP/DR)

1. Overview

The purpose of this Plan is to prepare fpPathfinder in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame. This includes:

- Data back-up and recovery (hard copy and electronic)
- Financial and operational assessments
- Alternate communications between fpPathfinder, customers, and employees
- Alternate physical location of employees

2. General Provisions

fpPathfinder's policy is to respond to a Significant Business Disruption (SBD) by safeguarding employees' lives and fpPathfinder property, making a financial and operational assessment, quickly recovering and resuming operations, protecting all of fpPathfinder's records, and allowing our customers to conduct business.

A. Significant Business Disruptions (SBDs)

fpPathfinder plan anticipates two kinds of SBDs: internal and external. Internal SBDs affect only fpPathfinder's ability to communicate and do business. External SBDs impact an entire region; this can include a terrorist attack, a city flood, or a wide-scale regional disruption. Our response to an external SBD relies more heavily on other organizations and systems.

B. Approval and Execution Authority

NAME/ROLE is responsible for approving the plan and for conducting the required annual review. Name/ROLE has the authority to execute this plan.

C. Plan Location and Access

fpPathfinder will maintain copies of this plan and the annual reviews, and the changes that have been made to it for inspection.

3. Emergency Contact Persons

fpPathfinder's emergency contact persons are:

Name: Michael Lecours
Phone: 860-748-1607
Email: mike@fppathfinder.com

4. Business Description

fpPathfinder, Inc. is a financial planning tool to help advisors have more diligent conversations with their clients about financial planning topics.

5. Office Location

In the event of an SBD, we will move our staff from affected office(s) to their homes. All employees have the ability to work remotely.

6. Data Back-Up and Recovery (Hard Copy and Electronic)

fpPathfinder maintains all records electronically in the cloud via known and approved cloud services and providers. fpPathfinder backs up electronic records daily. For the loss of electronic records, we will either:

- physically recover the storage media or electronically recover data from our back-up site, or

- if our primary site is inoperable, continue operations from our back-up site or an alternate location.

Restoration from back-up databases and other data is tested annually.

As fpPathfinder employs cloud services to ensure customer access to services, it is the responsibility of fpPathfinder personnel to ensure that the cloud services employed facilitate the resumption of service within acceptable timeframes. Service offerings should be selected and configured based on the capacity to facilitate resumption. Measures employed can include (but are not limited to):

1) Use of availability zones to ensure resumption of service at geographically distributed datacenters
2) Use of hot or cold sites
3) Mirroring services
4) Backup capabilities, provided that such capabilities allow for restoration within defined time windows

Where such mechanisms are not provided, fpPathfinder personnel will ensure that mitigations are in place to ensure resumption and that such mitigations are documented, available to personnel responsible for resumption tasks, and tested in a manner and at a frequency in line with this policy.

7. Alternate Communications Between fpPathfinder and Customers and Employees

A. Customers

In the event of an SBD, we will assess which means of communication are still available to us and use the means closest in speed and form (written or oral) to the means that we have used in the past to communicate. For example, if we have communicated with a party by email but the Internet is unavailable, we will call them on the telephone and follow up where a record is needed with paper copy in the U.S. mail.

B. Employees

In the event of an SBD, we will assess which means of communication are still available to us and use the means closest in speed and form (written or oral) to the means that we have used in the past to communicate.

8. Disclosure of the Plan

fpPathfinder has developed a Plan detailing how we will respond to events that significantly disrupt our business. Since the timing and impact of disasters and disruptions is unpredictable, we will have to be flexible in responding to actual events as they occur.

Planning – fpPathfinder intends to quickly recover and resume business operations after a significant business disruption and respond by safeguarding our employees and property, making a financial and operational assessment, protecting fpPathfinder’s books and records, and allowing our customers to continue to do business. In short, our plan is designed to permit fpPathfinder to resume operations as quickly as possible, given the scope and severity of the significant business disruption. Our plan addresses: data back-up and recovery; financial and operational assessments; alternative communications with customers and employees; and alternate physical location of employees.

Varying Disruptions – Significant business disruptions can vary in their scope and duration. For example, an event might target fpPathfinder alone, the building housing fpPathfinder, the business district where fpPathfinder is located, the city where we are located, the whole region, or globally. Within each of these areas, the severity of the disruption can also vary from minimal to severe.

In the case of a disruption to only fpPathfinder or our physical location, we will transfer our operations to a backup site as required and expect to recover and resume business as quickly as possible. In a disruption affecting our business district, city, or region, we will transfer our operations to a site outside of the affected area and recover and resume business within as quickly as possible. In either situation, we plan to continue in business and notify customers via the communication methods specified in this policy. If the significant business disruption is so severe that it prevents us from remaining in business, we will notify all customers as quickly as is economically and practically viable.

RTO and RPO – Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are critical values in business continuity planning. RPO refers to the amount of data that can be lost and still allow recovery to occur. RTO refers to the amount of time to restore business processes after an event to minimize impact. Given fpPathfinder' business as a customer-facing organization, these values are customer-driven as fpPathfinder services are used by customers to support their business processes. fpPathfinder has employed architectural models to facilitate rapid resumption of capability and to ensure minimal loss of data even during an event; however, fpPathfinder does not publish RTO or RPO values for the reasons listed above.

9. Updates and Annual Review

fpPathfinder will update this plan whenever we have a material change to our operations, structure, business or location. In addition, fpPathfinder will review this plan annually to modify it for any changes in our operations, structure, business or location.

10. Exceptions

This policy applies to all employees and contractors. Those found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

11. Responsibilities

It is the responsibility of all contractors, employees, and management to ensure that this policy is followed.

Teleworking Policy

1. Introduction

A teleworking arrangement is a voluntary agreement between the organization and the employee. It usually involves the employee working from home – either in a separate area of their living space, whether this is a house, apartment or other type of domestic residence – or in a location that is free of noise and that is conducive to performing business tasks.

The introduction of a teleworking arrangement, if managed effectively, has the potential to benefit both the individual and the organization. The individual will gain greater flexibility in working arrangements and possibly avoid a lengthy commute to and from an office. The organization is able to retain skilled and experienced staff whose circumstances suit teleworking and possibly save money on the rental, lease or purchase of office space.

This policy sets out the key information security-related elements that must be considered in agreeing a teleworking arrangement. It ensures that all of the necessary issues are addressed and that the organizations information assets are protected. This policy does not address the human resources aspects of teleworking such as health and safety, absence monitoring, job performance and contractual issues.

This policy applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to fpPathfinder systems.

From an information security point of view there are various aspects that need to be considered in each teleworking arrangement and the policy of the organization in these areas is set out in the following sections.

2. General Provisions

The organization's policy with regard to the provision of facilities to enable teleworking is detailed below.

2.1 Communications

In situations where networks containing sensitive information or critical devices will be accessed remotely, fpPathfinder may provide a physically separate communications link which is not connected in any way to existing personal communication channels. This is to ensure that:

- Network performance is not affected by other activities in the household
- The configuration of the router can be security-hardened according to organization policy
- The ability for other devices to connect to this link can be prevented

2.2 Securing Workplace

Employees must create a secure workspace, maintaining digital security, and by following the same best practices that you would in the office. Employees must:

- Stay current on software updates and patches.
- Never give someone else access to their work computer.
- Always protect your laptop by making sure it is password-protected, locked, and secure. Never leave it unattended. Do not disable automatic locking on your computer because you're at home.
- Ensure internet connection is secure by changing your router's default username and password to a unique password.
- Turn on encryption (WPA2 or WPA3) on your home router.

In situations where networks containing sensitive information or critical devices will be accessed remotely, fpPathfinder may also provide a physically separate communications link which is not connected in any way to existing personal communication channels. This is to ensure that:

- Network performance is not affected by other activities in the household
- The configuration of the router can be security-hardened according to organization policy
- The ability for other devices to connect to this link can be prevented through the protection of network keys etc.

2.3 Backup and Virus Protection

Where practical, no data will be stored on the client machine. In the event that this is unavoidable, it is the responsibility of the teleworker to ensure it is backed up and that it is protected.

Virus protection will be provided on all relevant equipment and configured to update automatically.

2.4 Technical Support

Technical support of all supplied equipment will be provided by IT Support.

2.5 Agreement Termination

In the event that the teleworking agreement is terminated for whatever reason, all equipment that was supplied as part of the arrangement must be returned to IT Support as soon as possible.

3. Exceptions

This policy applies to all employees and contractors. Those found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

4. Responsibilities

It is the responsibility of all contractors, employees, and management to ensure that this policy is followed.

Cryptographic Policy

1. Introduction

A key component in the set of controls used by organizations to protect classified, restricted, or scoped information is the use of cryptographic techniques. These techniques can be used to “scramble” data so that it cannot be accessed without the use of the appropriate key, to verify the integrity of messages and communications, to validate the origination and source of information, and for numerous other purposes.

Cryptographic controls can be used to achieve a number of information security-related objectives, including

- Confidentiality – ensuring that information cannot be read by unauthorized persons
- Integrity – proving that data has not been altered in transit or whilst stored
- Authentication – proving the identity of an entity requesting access to resources
- Non- repudiation – proving that an event did or did not occur or that a message was sent by an individual

The need for cryptographic controls will be highlighted from fpPathfinder risk assessment and will obviously not be applicable in all cases. However, where their use can provide the required level of protection, they should be applied according to the provisions set out in this policy.

This control applies to all systems, people and processes that constitute the organization’s information systems, including board members, directors, employees, suppliers and other third parties who have access to fpPathfinder systems.

In order to identify those areas in which the deployment of cryptographic techniques will be useful, fpPathfinder will take a managed approach as follows.

2. General Provisions

2.1 Risk Assessment

In general terms, the use of cryptography will be applicable in the protection of sensitive information (for example, data classified as “Confidential”). In addition, cryptography should be seriously considered in the following scenarios:

- On mobile devices such as laptops, tablets and smartphones
- For authorized use of removable media such as USB memory sticks
- Where classified data is transmitted across communications lines that extend beyond the boundaries of the organization (e.g., over the Internet)

2.2 Technique Selection

Once the general need for the use of cryptography has been identified by the risk assessment, a decision needs to be made about which specific techniques will be deployed. This will also involve the selection and possible purchase of software or hardware in order to implement the technique.

Note that the selection of such techniques must take into account any current regulations or national restrictions on the procurement and use of cryptographic technology which may affect the type, strength and quality of the encryption algorithm used.

In general, the policy of fpPathfinder is to use the following techniques for the relevant business process or situation:

Process/Situation	Technique	Specific Guidance
Financial information and PII gathering, storage and display	TLS version 1.3 if technically achievable or 1.2 if not	Certificates to be obtained from a reputable supplier. Cipher suites employed should be robust, using known strong algorithms and key lengths.
Protection of passwords on systems	All passwords must be protected against dictionary attacks, re-use, rainbow tables, and other known attacks. Selection of the appropriate strategy should account for current cryptographic best practices, for example employment of a salt, nonce, initialization vector or other method to prevent table-based attacks.	Use of legacy password hashing strategies (e.g., MD5) and/or techniques susceptible to dictionary attacks (e.g., SHA-256) should not be used. Use of known, trusted libraries (e.g., trusted implementations) are to be used where possible; in particular, FIPS 140-2 certified cryptosystems will be favored where possible.
Email Security	Symmetric/asymmetric encryption using S/MIME or equivalent	Features available in the relevant email client should be used to simplify the process
Remote Access	Virtual Private Network (VPN) using TLS when confidential information is accessed remotely.	An IPSec VPN or equivalent method (e.g., SSH port forwarding) may be used where permitted or when TLS VPN is not available

Table 1 Cryptographic techniques

The continued use of the specified techniques will be evaluated on each review of this policy.

2.3 Deployment

The deployment of cryptographic techniques must be managed carefully to ensure that the desired level of security is achieved. Where possible, more than one member of staff should be closely involved in the deployment in order to avoid both a single point of failure for support and to allow segregation of duties to take place.

Close consideration should be given to the on-going operation of the installed encryption so that documented operational procedures are fully in place and the relevant staff are trained in them.

2.4 Testing and Review

It is fpPathfinder policy to avoid any non-standard encryption methods where possible. By non-standard, we mean custom or in-house cryptomodule implementations. In the event that such usage is unavoidable, it is critical that the security of non-standard encryption methods be tested under as realistic conditions as possible to identify any weaknesses. Those techniques built into trusted implementations (e.g., TLS implementations or cryptographic routines/primitives/modules built into operating system platforms) may forgo such testing, but staff should routinely monitor for vulnerabilities in those platforms currently in use.

Where applicable, such testing should cover the use of:

- commonly-available software tools to try to break the encryption
- social engineering methods to try to discover the key
- interception of encrypted data at various points in its transmission

The results of tests will be formally reviewed, and lessons learned will be applied to the tested situation and communicated to other areas in which encryption is used in the organization.

3. Exceptions

This policy applies to all employees and contractors. Those found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

4. Responsibilities

It is the responsibility of all contractors, employees, and management to ensure that this policy is followed.