# Information Security Policy

## 1 Introduction

### 1.1 Purpose

Precision Concepts International (PCI) and its subsidiaries (collectively, “PCI”) strive maintain a working environment, both internally and through our suppliers, that conducts its personnel practices in line with the highest level of integrity and appropriate transparency. PCI operates in accordance with applicable laws and regulations and the company’s Code of Conduct. We recognize the importance of aligning our business practices with principles that not only comply with regulations but also transcend these standards to contribute positively to the well-being and further development of our workforce and communities.

Through this policy, we require all employees to act responsibly regarding the security of information, equipment, systems, as well as our communication abilities. This policy also outlines our objectives and sets forth the measures we are undertaking to ensure the promotion of responsible ethical practices and standards within our organization. It is a roadmap guiding all stakeholders – employees, suppliers, contractors, and our extended community – toward shared values and a collective commitment to responsible information management practices. This policy is informed by relevant internal and external expertise, is publicly available, and communicated internally and externally to all personnel, business partners and other relevant parties, and is reflected in operational procedures necessary to embed it throughout the business enterprise.

### 1.2 Material and Legal Scope

This policy applies to PCI’s employees, agents, contractors, and subcontractors in whatever capacity we employ them, regardless of the activities they conduct. This includes all our operational sites and locations where we conduct business activities. PCI will strive to ensure that its suppliers and business partners also adhere to the standards that are outlined within this policy.

### 1.3 Roles and Responsibilities

To ensure the effective implementation of this policy, PCI has assigned the following roles and responsibilities in the table below. These will ensure that all objectives and measures described in this policy are achieved to the best of our ability.

| Role | Responsibilities |
|---|---|
| Employees | Responsible for reading the following policy, acting in accordance with this policy, and reporting any (possible) breaches immediately. |
| Management | Responsible for communicating applicable measures throughout the company and providing the means to support their implementation. Management is also responsible for approving the contents herein. In addition, management will select a policy owner for each policy. |
| Policy Owner | Responsible for the implementation and monitoring of the policy. The contact officer must review and update the policy on an annual basis and respond to all requests and inquiries.<br>Name/Function: Mary Connery, VP of Human Resources<br>Contact details: mconnery@pcinternational.com |

## 2 Our Information Security Objectives

At PCI, we understand the importance of responsible information management and, as such, believe this should be incorporated into the basis of how we work as a company. Responsible information management includes, but is not limited to, the proper handling of client, customer, and employee data.

To ensure responsible information management, PCI has formalized the following:

- Comply with all relevant laws and regulations regarding information security in all geographies where we are present.
- Implement an incident response procedure to manage breaches of confidential information.
- Create a record retention schedule to facilitate efficient information management.
- Create and implement a stakeholder consent procedure for confidential information handling.

## 3 Our Information Security Measures

Specific measures regarding information security are outlined in detail below:

- We ensure continuous compliance with relevant local and international norms on information security and data protection for the countries in which we operate in.
- We handle confidential information with care and precaution, according to any applicable contractual obligations and confidentiality terms.
- We conduct cybersecurity training for our employees, which includes awareness to prevent any information security breaches.
- We have a whistleblower procedure / complaints mechanism in place to report information security concerns, accepting complaints from internal and external stakeholders.
- We require that no employee uses any of the Company's confidential or proprietary names, images, logos, pictures, or other information that is tied to the company on a blog, web page, social network or other social networking medium without prior permission of the company.

- No employee shall discuss any confidential or proprietary Company business on a blog, web page, social network, or social networking medium. All rules regarding confidentiality and proprietary business information apply in full to blogs, web pages, and social media. Any information that cannot be disclosed in a conversation cannot be disclosed in a blog, web page, or social media.
- Whether an employee is posting something on their own or someone else's blog, web page, social network or social media, if the person mentions the Company and expresses an opinion regarding the Company's politics or actions, the employee should include a disclaimer. The disclaimer should specifically state that the opinion expressed is the employee's personal opinion, and not that of the company.
- We require our employees to be respectful of their potential readers and colleagues and refrain from using harassing, defamatory, and discriminatory comments when making online comments about the Company, its managers, employees, contractors, and vendors.

# 4 Complaint Mechanism

## 4.1 Reporting Internally (Problem Solving Procedure)

PCI encourages anyone who sees something that might be in breach of this policy to report it, aligned with our Problem-Solving Procedure. Feel free to speak with your manager, Human Resources, or a manager of PCI if you witness or suspect any breach of this policy. The issue should first be discussed with the employee's supervisor or those directly involved in the matter. If the matter cannot be resolved:

- A meeting with the department manager or department director should be requested.
- If the matter remains unresolved, a meeting should be requested with Human Resources.

Any individual who believes they have encountered or witnessed a breach of this policy is strongly encouraged to report such concerns. We will ensure that no reporter faces retaliation or any adverse consequences for reporting a breach. We are committed to thoroughly investigating such reports and taking appropriate actions to address any confirmed violations.

In the case of any incident witnessed which may result in immediate incident, do not wait to start a formal reporting process. Instead, the witness should go directly to the person managing the activities or a senior staff member on shift to address the situation promptly. Determining what constitutes an emergency should be based on best judgment.

## 4.2 Reporting Externally (Whistleblower Hotline)

We encourage individuals to follow our Problem-Solving Procedure for concerns that can be dealt with in-house. However, should any individual need to make a report securely and confidentially, external reporting can also be undertaken using our External Hotline.

- **Subject Matter**: Anyone who believes that they have witnessed or experienced a violation of PCI's policies or suspects fraudulent behavior by an employee (at any level of the organization), supplier or contractor, can report it via the External Hotline. This can be done anonymously if the caller requests.

- **Reporting Procedures**: Calls can be made from any location at any time. Callers can choose to give their name or remain anonymous if they wish. All calls are documented and reported back to management, as appropriate.
- **Investigation Procedures**: Management will initiate an investigation into the matter and ensure proper resolution to the matter. If the reporter has not expressed the desire to remain anonymous, PCI will ensure that they remain informed about the process and outcome.
- **No Retaliation**: No officer, affiliate or employee of the company who in good faith reports a breach or wrongdoing will suffer harassment, retaliation, discipline or adverse employment consequence.

Reporting is available 24/7 and can be made via these channels:

By Phone: 855-400-6002; for Spanish - 800-216-1288
By email: standard-reports@mitratech.com
or go to: https://report.syntrio.com/pcinternational

Confidentiality will be maintained to the extent practical and permitted by law. Investigations will be conducted as confidentially as possible and related information will only be shared with others on a need-to-know basis. The investigation will be completed, and a determination made and communicated to the reporter as soon as practical.

### 4.3 Remediation Process

In accordance with the OECD Due Diligence Guidance for Responsible Business Conduct, PCI commits to providing or cooperating in remediation procedures where appropriate.

Some key elements of the remediation process through the lens of OECD include the following actions:

- Remedial Actions: If the investigation confirms wrongdoing, appropriate remedial actions will be taken. This may include disciplinary measures, corrective actions, and changes to policies or procedures to prevent future occurrences.
- Remedy to Victims: Should the wrongdoing reported result in damages to an individual, PCI will promptly address the situation by providing appropriate remedies. The type of remedy offered will depend on the nature and severity of the breach, ensuring fair and supportive measures are implemented to resolve the issue and support those affected.
- Reporting to Authorities: In cases where the wrongdoing may involve violations of laws or regulations, the findings may be reported to relevant authorities in compliance with legal obligations.
- Documenting and Reporting: The remediation process will be thoroughly documented, including investigation reports, actions taken, and outcomes. Relevant stakeholders, including company leadership, will be provided with regular updates on the company's efforts to address the reported concerns.

The ethics remediation process will follow all local laws and regulations. Impacts to the business operation will be addressed through outside counsel at the discretion of the VP of HR.

# 5 Policy Review, Sanctions & Approval

## 5.1 Policy Review

To ensure the continued validity and accuracy of this policy, an annual review will be carried out by the Policy Owner listed in Section 1.3 of this document. The review intends to identify any need for an update and make any necessary changes. The objectives and measures should be revised closely as these will almost certainly change periodically. If significant changes occur in PCI's operations, then a more frequent review of this document is advised.

## 5.2 Sanctions

All PCI members and affiliates are responsible for following this policy and applying it to their daily work. Further, managers are responsible for monitoring and ensuring that the personnel under their supervision follow this procedure. In the event of non-compliance with this policy, PCI reserves the right to corrective action against the perpetrator. In some instances, non-compliance may lead to relationship termination.

## 5.3 Approvals of the Latest Version of this Document

| Revision | Date | Description / Summary of Changes | Author |
|---|---|---|---|
| 000 | 08/01/2024 | <Initial Issue> | Harner, Amanda<br>HR OPS |
| 001 | 09/01/2026 | Changed branding and all instances of “Comar” to “PCI” | Mikayla Simphaly<br>Quality & Regulatory Engineer |

With the Acknowledgement and Approval of:

| | | |
|---|---|---|
| ELECTRONICALLY AUTHORIZED | DATE: | 09/24/26 |
| Mary Connery, VP of Human Resources | LOCATION: | Corporate |

Next Review: 09/01/2027