RESPONSIBLE DISCLOSURE POLICY

Sensitivity: Public

TABLE OF CONTENTS

1. CONTROL SECTION

MSC is maintaining this policy document to ensure that the guidance presented reflects the current control environment and aligns with management's objectives and business strategy.

Version	Date	Author	Verified	Approved	Comments/Notes
1.0	2024-SEP-27	IT Risk Management & Compliance Team	MSC Legal Team	MSC Global CISO	Final Release

2. INTRODUCTION

2.1 OVERVIEW

MSC aims to enhance the reporting process of security vulnerabilities through a controlled and structured model. This approach makes it easier for the sender to notify system vulnerabilities to the correct team inside MSC, following a defined approach, thereby contributing significantly to the security of ICT service sand preventing potential damage or disruptions. Responsible Disclosure involves reporting security vulnerabilities to the organization confidentially.

2.2 PURPOSE

The purpose of this Responsible Disclosure Policy is to provide a clear framework for security researchers, partners, and the general public to report vulnerabilities in MSC Cargo systems. This policy aims to encourage the responsible reporting of security vulnerabilities.

2.3 SCOPE

This policy applies to all security vulnerabilities identified by third parties in any of MSC Cargo systems, applications, or services.

3. POLICY

3.1 RESPONSIBLE DISCLOSURE PROCESS

- External researchers, partners, and the public are encouraged to report security vulnerabilities to cybersecurity@msc.com
- The security team will acknowledge receipt of vulnerability reports within 72 hours and notify the reporter via email.
- Assessment and Resolution: Reported vulnerabilities will be assessed, prioritized, and resolved based in their severity. The reporter will be kept informed of the progress within the first 10 days after the notification of the receipt of the vulnerability report.
- Following the responsible disclosure process, the reporter will be privately acknowledged for his contribution via email.

3.2 REPORTING PROCESS

To ensure a constructive process for both the reporter and MSC organization, MSC requests that individuals adhere to the following guidelines when reporting vulnerabilities:

1. Confidentiality: Report vulnerability to the following email: cybersecurity@msc.com
2. Detail: Provide detailed information to help MSC understand the nature and impact of the vulnerability.

   This includes:

   - A description of the vulnerability.
   - Steps to reproduce the issue.
   - Potential impact.
   - Any proof-of-concept code, if applicable.
3. Integrity: Any discovery and reporting must be done in good faith, avoiding actions that could harm MSC systems, data, or users. Do not exploit the vulnerability for any purpose other than testing.
4. Coordination: Do not publicly disclose the vulnerability. Following the responsible disclosure process, the reporter will be privately acknowledged for their contribution via email.

3.3 SAFE HARBOUR

To encourage responsible reporting, subject to the exclusion below MSC offers safe harbour to security researchers and reporters:

- Legal Protection: If the reporter identifies and reports a vulnerability in good faith, MSC will not pursue legal action against him for the vulnerability discovery.
- Confidentiality: MSC will not share reporter's personal information without his permission, except as required by law.
- Recognition: Following the responsible disclosure process, the reporter will be privately acknowledged for his contribution via email.

Excluded from the Safe Harbour, are the following acts that may lead to further action, including legal actions:

- Data destruction or alteration: Actions leading to data destruction or alteration.
- Denial of Service: Activities causing or attempting to cause a denial of service.
- Exploitation: Exploiting vulnerabilities beyond testing for the purpose of reporting.
- Privacy Violations: Accessing, copying, or deleting sensitive data, including personal data, beyond what is necessary to demonstrate the vulnerability.

3.4 CONFIDENTIALITY AND DATA PROTECTION

The reporter must treat all information about MSC systems, employees or costumers that comes into his possession or that he otherwise becomes aware of, which is not publicly available, as strictly confidential, and not share or otherwise use it for any purpose other than emailing it to us as a submission as described above.

If the reporter inadvertently accesses personal data on MSC system, he must immediately stop accessing the data, report this to the Security Team cybersecurity@msc.com and follow all further instructions from MSC. The reporter must follow the applicable data protection laws when reporting a vulnerability.

3.5 RECOGNITION PROGRAM

Following the responsible disclosure process, the reporter will be privately acknowledged for their contribution via email.

3.6 REVIEW AND UPDATE

This policy will be reviewed on yearly basis and updated as necessary to ensure its effectiveness and relevance.

3.7 APPROVAL

This policy is approved by the Chief Information Security Officer (Global CISO) and reviewed by the Team Legal.