



Medical Device Product Security Incident Response Guidance ^(MedPSIRG) for Medical Device Manufacturers in APAC



KNOWLEDGE PARTNER

ENSIGN
INFOSECURITY

H E A L T H D A T A

Contents

Overview of Medical Device Product Security Incident Response Guidance ([MedPSIRG](#)) for Medical Device Manufacturers in APAC

Medical Device Product Security Incident Response Framework ([MedPSIRF](#))

1. MedPSIRF Stakeholders and Their Roles


- 1.1. Executive Management
- 1.2. Product Development Team
- 1.3. Security Team (PSIRT - Product Security Incident Response Team)
- 1.4. IT Operations
- 1.5. Quality Management (QM)
- 1.6. Legal and Compliance
- 1.7. Public Relations (PR) and Communications
- 1.8. Customer Support

2. Services offered by the PSIRT

- 2.1. Stakeholder Ecosystem Management
- 2.2. Vulnerability Reporting and Disclosure
- 2.3. Remediation
- 2.4. Training and Education



Medical Device Product Security Incident response Plan (MedPSIRP)

- 
1. **MedPSIRP Stakeholders and Their Roles**
 - 1.1. Executive Management
 - 1.2. Product Development Team
 - 1.3. Security Team (PSIRT - Product Security Incident Response Team)
 - 1.4. IT Operations
 - 1.5. Quality Management (QM)
 - 1.6. Legal and Compliance
 - 1.7. Public Relations (PR) and Communications
 - 1.8. Customer Support
 - 1.9. Incident Commander
 - 1.10. Incident Response Program Manager
 - 1.11. Incident Response Analyst
 2. **Incident Response Plan Overview**
 3. **Incident Response Process-Specific Definitions**
 4. **CVE (Common Vulnerabilities and Exposures)**
 5. **CVSS Score (Common Vulnerability Scoring System)**
 6. **Common Weakness Enumeration (CWE)**
 7. **Embargo**
 8. **Incident Response Process**
 9. **Communication**
 10. **Example Incident: Firmware Vulnerability in a Medical Device**

Overview of Medical Device Product Security Incident Response Guidance (**MedPSIRG**) for Medical Device Manufacturers in APAC

This Medical Device Product Security Incident Response Guidance (**MedPSIRG**) aims to provide medical device manufacturers guidance on the considerations needed when establishing functions to collect, triage, remediate and report on discovered product vulnerabilities. To this end, a framework and a plan for medical device product security incident response are offered. Drawing on established industry principles and practices, this document aims to assist organizations in effectively managing and responding to security vulnerabilities in medical devices.

This **MedPSIRG** guidance document serves as a foundational tool for medical device manufacturers to build, maintain, and enhance their product security incident response capabilities, ensuring the safety and security of their products and the protection of patients and users.

This **MedPSIRG** comes in two parts. They are:

a. A Medical Device Product Security Incident Response Framework (**MedPSIRF**)

The **MedPSIRF** outlines the minimum services Product Security Incident Response Team (PSIRTs) should provide their organisation and customers. This **MedPSIRF** aims to support organizations in building, maintaining, and enhancing the capabilities of their PSIRTs. Along with the minimum services, it lists the stakeholder and their associated roles. To aid understanding, contextualised examples are provided. Further guidance is provided by mapping the stakeholders and the role of each service, allowing teams to tailor their approaches to meet their own organisation and customer needs.

b. A Medical Device Product Security Incident Response Plan (**MedPSIRP**)

This **MedPSIRP** focuses on offering a method of rating the severity of a discovered vulnerability, the actions that proceed after, and the communication activities to inform affected parties. To this end, this Plan sets the baseline for classifying vulnerability severity, guiding the response efforts to mitigate risks to the Company, its customers, and the broader ecosystem. This **MedPSIRP** aims to support coordination among stakeholders, guide the response process from initial vulnerability discovery to resolution, including a retrospective review for continuous improvement. It offers an overview of the processes for reporting, triaging, remediating and fixing vulnerabilities.

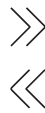


FRAMEWORK

Discusses “what” is needed and “why”

Example:

Organisations must establish a comprehensive communications plan to promptly inform relevant stakeholders during incidents or crises (“what”), thereby mitigating the risk of misinformation and preventing unnecessary panic (“why”).



PLAN

Discusses “how” to provide guidelines on implementing the framework

Example:

When an incident occurs, following the communications plan, specific messages need to be sent out to inform both internal stakeholders (e.g. product engineering, IT operations, QM team) and external stakeholders (e.g. affected customers, regulatory bodies, media).

Medical Device Product Security Incident Response Framework (MedPSIRF)

The **MedPSIRF** outlines the minimum services Product Security Incident Response Team (PSIRTs) should provide their organisation and customers. This **MedPSIRF** aims to support organizations in building, maintaining, and enhancing the capabilities of their PSIRTs. Along with the minimum services, it lists the stakeholder and their associated roles. To aid understanding, contextualised examples are provided. Further guidance is provided by mapping the stakeholders and the role of each service, allowing teams to tailor their approaches to meet their own organisation and customer needs.

1. MedPSIRF Stakeholders and Their Roles



The stakeholders and their associated roles identified here are included in both the **MedPSIRF** and **MedPSIRP** and are from the perspective of implementing the **MedPSIRP**. Hence, the language used is tactical in nature. It aims to outline the stakeholder roles and responsibilities to support coordinated, concerted and, unified response to security incidents affecting medical devices. By delineating specific duties for each stakeholder, the framework enhances communication, accountability, and collaboration. This in turn supports rapid identification and remediation of security vulnerabilities, minimises potential risks, and ensures compliance with regulatory requirements. Furthermore, it builds trust with customers and stakeholders by demonstrating a commitment to proactive and effective incident management leading to the preservation of safety and security in medical devices. Organisations may choose to involve more stakeholders (e.g. medical affairs officer) where feasible.

1.1. Executive Management

- **Role:** Oversight and decision-making authority.
- **Responsibilities:**
 - Approve the PSIRP and ensure it aligns with corporate policies and regulatory requirements.
 - Provide necessary resources and support for incident response activities.
 - Communicate with regulatory bodies, partners, and customers as needed during major incidents.

1.2. Product Development Team

- **Role:** Design, develop, and maintain medical devices.
- **Responsibilities:**
 - Incorporate and test security controls in the product development lifecycle to mitigate weaknesses and vulnerabilities in products.
 - Collaborate with the security team to address identified vulnerabilities.
 - Implement, test and support deployment of security patches and updates.

1.3. Security Team (PSIRT - Product Security Incident Response Team)

- **Role:** Manage and coordinate the response to security incidents.
- **Responsibilities:**
 - Monitor for potential security threats and vulnerabilities.
 - Conduct initial triage and assessment of reported vulnerabilities.
 - Lead the incident response process, including containment, remediation, and recovery.
 - Maintain and update the PSIRP.

1.4. IT Operations

- **Role:** Maintain IT infrastructure and support services.
- **Responsibilities:**
 - Ensure the availability and security of IT systems and networks.
 - Assist in the investigation and mitigation of security incidents.

1.5. Quality Management (QM)

- **Role:** Ensure product quality and compliance.
- **Responsibilities:**
 - Conduct security testing as part of the product release process.
 - Report security issues identified during testing.

1.6. Legal and Compliance

- **Role:** Ensure compliance with legal and regulatory requirements.
- **Responsibilities:**
 - Advise on regulatory requirements related to product security and incident response.
 - Manage communication with regulatory bodies and ensure timely reporting of incidents.
 - Ensure that all incident response activities comply with applicable laws and regulations.

1.7. Public Relations (PR) and Communications

- **Role:** Manage external communication.
- **Responsibilities:**
 - Develop and execute communication plans during security incidents.
 - Coordinate public disclosures and media interactions.
 - Ensure consistent and accurate messaging to stakeholders.

1.8. Customer Support

- **Role:** Provide support to customers and users.
- **Responsibilities:**
 - Communicate with customers regarding security incidents and remediation steps.
 - Provide technical support to customers during incident resolution.
 - Collect and relay customer feedback to the incident response team.

2. Services offered by the PSIRT

The service areas outlined here are the core functions of a PSIRT. They are performed by the PSIRT to effectively engage with internal and external stakeholders. These services are active throughout the incident lifecycle and the PSIRT's maturity process, ensuring all stakeholders are well-informed and involved in the incident response.

2.1. Stakeholder Ecosystem Management

Description: Effective management of stakeholders is crucial for a coordinated and efficient incident response. This involves clear definition and communication of roles and responsibilities among internal teams, as well as active engagement with external partners and regulatory bodies. Ensuring stakeholders are informed and involved throughout the incident lifecycle helps in swift decision-making and action.

2.1.1 Internal Stakeholder Management

Description: Identifying and defining roles for key internal stakeholders, including security, product development, and executive teams, to ensure effective collaboration across all phases of the product incident response.

Example: During an incident where a vulnerability is discovered in a pacemaker, the security team handles the initial triage and assessment, the product development team works on remediation, and the executive team manages communication with regulatory bodies such as Singapore's Health Sciences Authority (HSA).

Stakeholder Roles:

- **Security Team:** Receives and logs the vulnerability report, assigns a lead, and conducts the initial assessment.
- **Executive Management:** Provides oversight and ensures necessary resources are allocated.
- **Product Development Team:** Assesses the technical impact and develops remediation plans.
- **IT Operations:** Supports infrastructure needs for assessment and remediation.

2.1.2 Community and Organizational Engagement

Description: Establishing partnerships with industry bodies, regulatory agencies, and cybersecurity communities enhances threat intelligence and best practices sharing.

Example: Joining the local medical device manufacturer's association, such as APACMed, and participating in their cybersecurity task force can provide insights into the latest threats and regulatory changes.

Stakeholder Roles:

- **Security Team:** Leads engagement with external entities and gathers threat intelligence.
- **Executive Management:** Provides strategic direction and approvals for external partnerships.
- **Legal and Compliance:** Ensures that all engagements comply with regulatory requirements.

2.1.3 Incident Communications Coordination

Description: Developing a communication plan outlining internal and external communication protocols ensures consistent and clear messaging, minimising misinformation and panic.

Example: During a data breach involving patient information, the communication plan guides the team on how to inform affected patients, regulatory bodies, and the media.

Stakeholder Roles:

- **Security Team:** Provides technical details and incident updates.
- **Public Relations (PR) and Communications:** Drafts and coordinates public statements and internal updates.
- **Legal and Compliance:** Reviews communications to ensure they comply with regulations.
- **Executive Management:** Approves communication strategies and statements.

2.1.4 Stakeholder Metrics

Description: Defining metrics to measure stakeholder engagement and response efficiency provides insights into the effectiveness of the incident response process and identifies areas for improvement.

Example: Metrics such as the time taken to acknowledge a reported vulnerability, the number of stakeholders informed within the first hour, and the speed of patch deployment can be tracked and analysed.

Stakeholder Roles:

- **Security Team:** Collects and analyses engagement and response metrics.
- **Executive Management:** Reviews metrics and provides feedback for process improvements.
- **Product Development Team:** Implements process improvements based on metric analysis.
- **Legal and Compliance:** Ensures that metric collection and reporting comply with regulatory standards.

2.2. Vulnerability Reporting and Disclosure

Description: Establishing processes for reporting and disclosing vulnerabilities is essential for maintaining product security and trust. This includes setting criteria for reportable vulnerabilities, tracking discovery metrics, triaging, and analysing reports, and ensuring transparent communication about discovered vulnerabilities.

2.2.1 Eligibility Criteria

Description: Establishing clear criteria for what constitutes a reportable vulnerability ensures only relevant vulnerabilities are reported, preventing resource wastage.

Example: Criteria might include the potential impact on patient safety, data integrity, and system functionality.

Stakeholder Roles:

- **Security Team:** Defines and updates eligibility criteria.
- **Product Development Team:** Provides technical input on impact and relevance.
- **Quality Management:** Reviews eligibility criteria
- **Legal and Compliance:** Ensures criteria meet regulatory and legal standards.

2.2.2 Vulnerability Discovery Metrics

Description: Tracking metrics such as time to discovery, time to report, and sources of vulnerability reports helps in improving the vulnerability discovery processes.

Example: Metrics might show that vulnerabilities reported by third-party researchers are typically more critical than those discovered internally.

Stakeholder Roles:

- **Security Team:** Collects and analyses discovery metrics.
- **Product Development Team:** Provides input on discovery sources and impact.

2.2.3 Vulnerability Triage and Analysis

Description: Implementing a triage process to prioritise vulnerabilities based on severity and impact ensures critical vulnerabilities are addressed promptly, reducing potential risks.

Example: A vulnerability affecting the firmware of an infusion pump might be prioritised over a non-critical software bug in a patient management application.

Stakeholder Roles:

- **Security Team:** Conducts initial assessment and prioritises vulnerabilities.
- **Product Development Team:** Provides technical validation and analysis.
- **QM Team:** Assists in prioritisation based on testing results.

2.2.4 Vulnerability Reporting

Description: Setting up a secure and accessible vulnerability reporting channel for internal and external reporters encourages prompt and accurate reporting of vulnerabilities in line with regulatory requirements.

Example: An online portal with options for anonymity and encryption can facilitate secure reporting from researchers and internal staff.

Stakeholder Roles:

- **Security Team:** Manages the reporting channel and documents reports.
- **IT Operations:** Ensures the security of the reporting channel.
- **Legal and Compliance:** Reviews reports for regulatory compliance.

2.2.5 Information on Bounties or Acknowledgments Offered

Description: Implementing a vulnerability reward program or acknowledging contributors publicly motivates researchers and stakeholders to report vulnerabilities responsibly.

Example: Offering financial rewards or public recognition for reported vulnerabilities can incentivise more thorough reporting.

Stakeholder Roles:

- **Security Team:** Evaluates the severity and impact of reported vulnerabilities.
- **Executive Management:** Approves rewards based on evaluations.
- **Legal and Compliance:** Ensures the reward program complies with regulations.
- **Public Relations (PR) and Communications:** Publicises acknowledgments and rewards.

2.2.6 Guidelines on How Vulnerabilities are Publicly Disclosed

Description: Developing a disclosure policy specifying timelines and conditions for public disclosure aligned with pre-existing regulatory requirements ensures transparency while protecting users until a fix is available.

Example: A policy might state that vulnerabilities will be publicly disclosed 90 days after reporting unless a fix is available sooner.

Stakeholder Roles:

- **Security Team:** Recommends disclosure timelines based on assessments.
- **Executive Management:** Approves disclosure timelines.
- **Legal and Compliance:** Ensures compliance with regulatory requirements.
- **Public Relations (PR) and Communications:** Drafts and coordinates public statements.

2.2.7 Identifying Unreported Vulnerabilities

Description: Conducting regular security audits and assessments proactively identifies vulnerabilities that might not have been reported.

Example: Performing a penetration test on a new medical device firmware before release can uncover potential vulnerabilities.

Stakeholder Roles:

- **Security Team:** Leads the planning and execution of audits.
- **Product Development Team:** Provides technical support during audits.
- **Third-Party Auditors:** Conducts independent assessments.

2.2.8 Monitoring for Product Component Vulnerabilities

Description: Continuously monitoring third-party components and dependencies for vulnerabilities ensures timely updates and patches, maintaining overall product security.

Example: Regularly checking the National Vulnerability Database (NVD) for vulnerabilities in third-party libraries used in medical devices.

Stakeholder Roles:

- **Security Team:** Manages monitoring tools and processes.
- **IT Operations:** Supports the integration of monitoring tools.
- **Product Development Team:** Provides input on third-party components.

2.3. Remediation

Description: Developing processes to promptly address identified vulnerabilities ensures the security and functionality of medical devices. This includes managing security patches, handling incidents effectively, and tracking remediation efforts through metrics.

2.3.1 Security Patch Release Management

Description: Establishing a patch management process to prioritise and deploy security patches ensures vulnerabilities are promptly fixed, maintaining device security.

Example: Creating a schedule for regular patch updates and emergency patches for critical vulnerabilities.

Stakeholder Roles:

- **Security Team:** Identifies and prioritises patches.
- **Product Development Team:** Develops patches based on priorities.
- **QM Team:** Validates patches before deployment.
- **IT Operations:** Ensures infrastructure readiness for patch deployment.

2.3.2 Incident Handling

Description: Developing incident handling procedures detailing steps from detection to resolution in line with regulatory requirements provides a clear and structured approach to managing security incidents.

Example: Creating a step-by-step guide for handling a ransomware attack on a medical device management system.

Stakeholder Roles:

- **Security Team:** Detects and logs the incident, leads the investigation, and coordinates remediation.
- **IT Operations:** Assists in containment and forensic analysis.
- **Product Development Team:** Provides technical fixes for mitigation and recovery.
- **Executive Management:** Provides oversight and ensures necessary resources.
- **Legal and Compliance:** Ensures documentation and compliance with regulations.

2.3.3 Vulnerability Release Metrics

Description: Tracking metrics such as time to patch, number of patches released, and patch adoption rate measures the effectiveness of the remediation process and identifies areas for improvement.

Example: Analysing the average time to deploy patches across different device types to identify bottlenecks.

Stakeholder Roles:

- **Security Team:** Collects and analyses remediation metrics.
- **Product Development Team:** Provides input on patch deployment.
- **QM Team:** Contributes validation data.
- **Executive Management:** Reviews metrics and provides feedback for process improvements.

2.4. Training and Education

Description: Providing continuous training and education for the PSIRT and development teams, as well as all stakeholders, ensures preparedness and a security-first culture. This includes regular training sessions, ongoing security awareness programs, and incorporating lessons learned into future training.

2.4.1 Training the PSIRT and Development Teams

Description: Providing regular training on the latest security threats, vulnerability management, and incident response techniques ensures the team is well-prepared to handle security incidents effectively.

Example: Conducting quarterly training sessions on new cybersecurity threats specific to medical devices.

Stakeholder Roles:

- **Security Team:** Provides training on detection, analysis, and remediation.
- **Product Development Team:** Participates in training on secure coding practices.
- **QM Team:** Participates in training on testing and validation.
- **Executive Management:** Supports and promotes training programs.

2.4.2 Continuing Education for All Stakeholders

Description: Offering ongoing security awareness programs for all employees promotes a security-first culture within the organisation.

Example: Implementing monthly cybersecurity awareness training sessions for all staff, focusing on phishing, social engineering, and secure handling of patient data.

Stakeholder Roles:

- **Security Team:** Provides training on security awareness.
- **All Employees:** Participate in awareness training sessions.
- **Executive Management:** Supports and promotes training programs.
- **Legal and Compliance:** Ensures training content complies with regulations.

Medical Device Product Security Incident Response Plan (MedPSIRP)

This **MedPSIRP** focuses on offering a method of rating the severity of a discovered vulnerability, the actions that proceed after, and the communication activities to inform affected parties. To this end, this **MedPSIRP** sets the baseline for classifying vulnerability severity, guiding the response efforts to mitigate risks to the Company, its customers, and the broader ecosystem. This **MedPSIRP** aims to support coordination among stakeholders, guide the response process from initial vulnerability discovery to resolution, including a retrospective review for continuous improvement. It offers an overview of the processes for reporting, triaging, remediating and fixing vulnerabilities.

1. MedPSIRP Stakeholders and Their Roles

The stakeholders and their associated roles identified in the **MedPSIRP** include both the roles listed in the **MedPSIRF** and an extended list of roles typically needed for the team. Hence, the language used is tactical in nature. It aims to further outline the tactical roles and responsibilities to support coordinated, concerted and, unified response to security incidents affecting medical devices. It further reinforces commitment to proactive and effective incident management and transparency in communication leading to the preservation of safety and security in medical devices.

1.1. Executive Management

- **Role:** Oversight and decision-making authority.
- **Responsibilities:**
 - Approve the MedPSIRP.
 - Ensure alignment with corporate policies and regulatory requirements.
 - Provide necessary resources, and communicate with regulatory bodies, partners, and customers during major incidents.

1.2. Product Development Team

- **Role:** Design, develop, and maintain medical devices.
- **Responsibilities:**
 - Integrate security best practices into the product development lifecycle.
 - Collaborate with the security team to address identified vulnerabilities.
 - Implement and test security patches and updates.

1.3. Security Team (PSIRT - Product Security Incident Response Team)

- **Role:** Manage and coordinate the response to security incidents.
- **Responsibilities:**
 - Monitor for potential security threats and vulnerabilities.
 - Conduct initial triage and assessment of reported vulnerabilities.
 - Lead the incident response process including containment, remediation, and recovery, and maintain and update the MedPSIRP.

1.4. IT Operations

- **Role:** Maintain IT infrastructure and support services.
- **Responsibilities:**
 - Support the deployment of security patches and updates.
 - Ensure the availability and security of IT systems and networks.
 - Assist in the investigation and mitigation of security incidents.

1.5. Quality Management (QM)

- **Role:** Ensure product quality and compliance.
- **Responsibilities:**
 - Test and validate security patches and updates before deployment.
 - Conduct security testing as part of the product release process.
 - Report security issues identified during testing.

1.6. Legal and Compliance

- **Role:** Ensure compliance with legal and regulatory requirements.
- **Responsibilities:**
 - Advise on regulatory requirements related to product security and incident response.
 - Manage communication with regulatory bodies.
 - Ensure that all incident response activities comply with applicable laws and regulations.

1.7. Public Relations (PR) and Communications

- **Role:** Manage external communication.
- **Responsibilities:**
 - Develop and execute communication plans during security incidents.
 - Coordinate public disclosures and media interactions.
 - Ensure consistent and accurate messaging to stakeholders.

1.8. Customer Support

- **Role:** Provide support to customers and users.
- **Responsibilities:**
 - Communicate with customers regarding security incidents and remediation steps.
 - Provide technical support to customers during incident resolution.
 - Collect and relay customer feedback to the incident response team.

1.9. Incident Commander

- **Role:** Technical focal point and decision-maker during major incidents.
- **Responsibilities:**
 - Delegate tasks.
 - Coordinate investigation actions and resources.
 - Ensure resolution of the incident.

1.10. Incident Response Program Manager

- **Role:** Manage and orchestrate incidents from beginning to end.
- **Responsibilities:**
 - Track incidents.
 - Establish communication channels
 - Maintain coordination documents and prepare executive briefings.

1.11. Incident Response Analyst

- **Role:** Conduct initial triage of all incoming incidents.
- **Responsibilities:**
 - Review and organise collected data.
 - Create vulnerability tasks and ensure accurate documentation.

2. Incident Response Plan Overview

The Incident Response Plan (IRP) outlines the structured approach the company uses to manage and respond to security vulnerabilities. It details the orchestration process, classification of severity levels, and coordination of efforts necessary to address incidents effectively. The plan ensures timely communication and coordination among stakeholders and provides a high-level process from inception to closure, including a retrospective review for continuous improvement.

3. Incident Response Process-Specific Definitions

1. Flaw

A weakness or vulnerability within the system that needs remediation, documented with all necessary details for tracking and resolution.

2. Major Incident

An incident with significant impact, such as high severity, ease of exploitation, or high visibility, requiring coordinated response across the organisation.

3. Minor Incident

An incident with lower impact and risk, requiring standard response procedures without extensive coordination.

4. Orchestration

The coordination and communication between stakeholders to manage and respond to security incidents effectively.

- | | |
|--|--|
| <p>5. Task
A unit of work identified during incident response, requiring further assessment and resolution.</p> | <p>6. Vulnerability
A security flaw in an asset that increases the risk of a threat.</p> |
| <p>7. Weakness
A defect in software or hardware that could be exploited if not addressed.</p> | <p>8. Security Bulletin (SB)
A public-facing document providing detailed information about a major incident</p> |
| <p>9. Security Advisory (SA)
A document containing security fixes for vulnerabilities, approved, and released in a timely manner.</p> | |

4. CVE (Common Vulnerabilities and Exposures)

CVE is a list of publicly disclosed cybersecurity vulnerabilities; each assigned a unique identifier. It provides a standardised method for identifying vulnerabilities and sharing information across the industry. The company may act as a CVE Numbering Authority (CNA) to assign CVE IDs and ensure accurate descriptions and references.

5. CVSS Score (Common Vulnerability Scoring System)

CVSS is a standardised framework for assessing the severity of security vulnerabilities. It provides a numerical score representing the impact and exploitability of a vulnerability. The company uses CVSS to determine the severity level and prioritise remediation efforts.

6. Common Weakness Enumeration (CWE)

CWE is a list of software and hardware weakness types, providing a common language for identifying and describing vulnerabilities. It helps in understanding the nature of weaknesses and improving development practices to mitigate risks.

7. Embargo

An embargo restricts the public disclosure of a vulnerability, allowing time for the organisation to develop and test fixes before releasing information. It ensures that sensitive information is shared only with key stakeholders who need to know and can assist in the remediation process.

8. Incident Response Process +

This Incident Response Process detailed outlines the essential 4 phases of Notification & Triage, Assessment & Coordination, Remediation & Release, and Recovery & Closure. The aim of these phases ensures Medical Device Manufacturers evaluate incoming security concerns, assess severity and impact, plan possible mitigations, tests fixes, document all incidents and communication clearly to all stakeholders across the incident and include a retrospective review for process improvement.



1. Notification & Triage

- **Description:** The Notification & Triage phase focuses on the intake and initial triage of the task. This initial triage process determines any effects on the company's components and offerings, assigning a unique Common Vulnerability and Exposures (CVE) number to each vulnerability, establishing an internal Common Vulnerability Scoring System (CVSS) score, identifying the vulnerability type/family through the Common Weakness Enumeration (CWE) classification, and assigning a severity rating to each product affected by the CVE for passing to Product Engineering.
- **Example:** A vulnerability is discovered in a medical device's firmware. The PSIRT assigns a CVE number, calculates the CVSS score, classifies the vulnerability using CWE, and determines the severity level. Initial documentation is created, and the vulnerability is logged for further assessment.

2. Assessment & Coordination

- **Description:** The Incident Response continues with a formal assessment of the vulnerability. This process includes the validation of the vulnerability, confirming the company's severity level, and identifying possible mitigations/remediations. During this phase, Incident Response analysts initiate the drafting of documentation providing a technical explanation of the vulnerability and forming potential remediation options. The Product Engineering team is officially informed, and the coordination process begins.
- **Example:** The vulnerability in the medical device's firmware is formally assessed. The severity is confirmed, and potential mitigations are identified. The Product Engineering team is notified and provided with detailed documentation. Coordination efforts begin to plan the remediation strategy.

3. Remediation & Release

- **Description:** Secure Engineering drives the company's remediation efforts by orchestrating the overall vulnerability remediation timelines and ensuring they align with the appropriate SLAs for all key stakeholders involved. Product Engineering organisation determines the proper remediation for the vulnerability and ensures the documentation of appropriate controls to mitigate the risk of the vulnerability. Quality Engineering tests the remediation and ensures it addresses the vulnerability without introducing new issues. The final build of the code is prepared for public release, and all necessary internal and external communications are coordinated.
- **Example:** The Product Engineering team develops a patch for the firmware vulnerability. Quality Engineering validates the patch, and the release team prepares the final build. Communication plans are executed to inform stakeholders, and the patch is deployed to affected devices.

4. Recovery & Closure

- **Description:** The Incident Response organisation concludes the incident response efforts, ensuring final tracking of the incident, internal and external communications are properly developed, reviewed, and released, and follow-up activities are completed. A retrospective review is conducted to identify lessons learned and areas for improvement in the process, which are then integrated into future incident response efforts.
- **Example:** After the firmware patch is deployed, the incident response team finalises all documentation and communications. A retrospective review identifies areas for improvement, such as enhancing initial triage procedures. These improvements are documented and implemented for future incidents.

9. Communication

Importance of Clear Communication Effective communication is critical throughout the incident response process. Clear, timely, and accurate communication ensures that all stakeholders are informed and coordinated, minimising the impact of the incident, and maintaining trust with customers and regulatory bodies.

1. Internal Communication

- **Description:** Keep all internal stakeholders informed about the incident status, actions taken, and next steps. Regular updates ensure that everyone is aligned and can respond effectively.
- **Example:** During the firmware vulnerability incident, the PSIRT provides regular updates to the executive management, Product Engineering, IT Operations, QM Team, and other relevant internal stakeholders.

2. External Communication

- **Description:** Communicate with external stakeholders, including customers, regulatory bodies, and the media, in a transparent and consistent manner. Provide timely updates on the incident, remediation efforts, and any potential impact on users.
- **Example:** The PR and Communications team coordinates with the Legal and Compliance team to draft and release statements to affected customers, regulatory bodies, and the media about the firmware vulnerability and the steps taken to resolve it.

3. Communication Plans

- **Description:** Develop and execute comprehensive communication plans for both internal and external stakeholders. These plans should include protocols for incident notification, regular updates, and post-incident communication.
- **Example:** : A communication plan is developed for the firmware vulnerability incident, outlining the specific messages, timing, and channels for communicating with internal teams, customers, regulatory bodies, and the media.

10. Example Incident: Firmware Vulnerability in a Medical Device

To illustrate the use of the Incident Response Process, consider an example where a vulnerability is discovered in the firmware of a medical device that could potentially allow unauthorised access to patient data. This example hopes to demonstrate the key phases and key activities performed by stakeholders to support systematic and effective response to security incidents, safeguarding the integrity of the medical products.

1. Notification & Triage

- The Security Team (PSIRT) receives a report of the vulnerability from a security researcher.
- The PSIRT assigns a CVE number, calculates the CVSS score, and classifies the vulnerability using CWE.
- The severity level is determined to be high due to the potential impact on patient data.
- Initial documentation is created, and the vulnerability is logged for further assessment.

2. Assessment & Coordination

- The PSIRT conducts a formal assessment of the vulnerability, confirming its validity and severity.
- Possible mitigations and remediation strategies are identified.
- The Product Engineering team is notified and provided with detailed documentation about the vulnerability.
- Coordination efforts begin to plan the remediation strategy, including regular meetings between the PSIRT, Product Engineering, IT Operations, and QM Team.

3. Remediation & Release

- The Product Engineering team develops a patch to address the firmware vulnerability.
- Quality Engineering validates the patch to ensure it resolves the vulnerability without introducing new issues.
- The release team prepares the final build for deployment.
- Communication plans are executed to inform all stakeholders, including internal teams, customers, and regulatory bodies, about the upcoming patch and its deployment schedule.
- The patch is deployed to all affected devices.

4. Recovery & Closure

- The Incident Response team ensures final tracking of the incident, documenting all actions taken and communications made.
- A retrospective review is conducted to identify lessons learned and areas for improvement in the incident response process.
- Improvements are documented and implemented for future incidents.

5. Communication

- **Internal Communication:** Regular updates are provided to executive management, Product Engineering, IT Operations, QM Team, and other relevant internal stakeholders throughout the incident response process.
- **External Communication:** The PR and Communications team, in coordination with the Legal and Compliance team, drafts and releases statements to affected customers, regulatory bodies, and the media. These statements provide details about the vulnerability, the remediation steps taken, and the impact on users.
- **Communication Plans:** A comprehensive communication plan is developed and executed, outlining the specific messages, timing, and channels for communicating with internal and external stakeholders.

Authors & Contributors

APACMed Secretariat

Su Fen Ong

Lead, Health Data & AI, APACMed

Authors

Leonard Koh

Head, Crisis Operations and Training, Ensign InfoSecurity, CISA, CDPSE, OXELP

Yeo Quan Ren

Consultant, Crisis Operations and Training, Ensign InfoSecurity, MSc, MBA

Contributors

Asok Kumar Raghavan Nair

Quality and Regulatory Director, Global Strategic Regulatory Affairs, Abbott

Jagathesh Rajavasagam

Risk and Cybersecurity Officer, APAC, Abbott

James Chan

Regulatory Affairs Director, APAC, Varian Medical Systems

Joern Lubadel

Global Head of Product Security, B. Braun Group

Juan Gomez

Regional ICT Director, APAC, Terumo

Paul Chua

Cybersecurity Officer, Greater Asia, BD

Stefan Gentsch

Cybersecurity Officer, Asia Pacific, Siemens Healthineers



About Ensign



Ensign InfoSecurity is the largest comprehensive cybersecurity service provider in Asia. Headquartered in Singapore, Ensign offers bespoke solutions and services to address their clients' cybersecurity needs. Their core competencies are in the provision of cybersecurity advisory and assurance services, architecture design and systems integration services, and managed security services for advanced threat detection, threat hunting, and incident response. Underpinning these competencies is in-house research and development in cybersecurity. Ensign has two decades of proven track record as a trusted and relevant service provider, serving clients from the public and private sectors in the Asia Pacific region.



About APACMed

The Asia Pacific Medical Technology Association (APACMed) represents manufacturers and suppliers of medical equipment, devices and in vitro diagnostics, industry associations, and other key stakeholders associated with the medical technology industry in the Asia Pacific region. APACMed's mission is to improve the standards of care for patients through innovative collaborations among stakeholders to jointly shape the future of healthcare in Asia-Pacific. For more information, visit www.apacmed.org