IMRICOR MEDCIAL SYSTEMS, INC.

INFORMATION AND DATA PROCESSING SECURITY POLICY

1 Purpose

This policy ensures that all data processing activities within Imricor Medical Systems, Inc. (**Imricor**) adhere to the highest security standards, aligning with ISO 27001 and ISO 27002 frameworks to protect the confidentiality, integrity, and availability of information assets. By implementing robust security measures, Imricor seeks to mitigate risks associated with data breaches, unauthorized access, and data loss. Additionally, this policy aims to foster a culture of security awareness and responsibility among all employees and stakeholders.

2 Scope

This policy applies to all employees, contractors, third parties, and stakeholders involved in handling, processing, storing, and transmitting data within Imricor. It covers all types of data, including personal, corporate, financial, and customer-related information. The policy extends to all technology systems, applications, cloud services, and physical storage devices utilized by Imricor.

3 Information Security Management System (ISMS)

Imricor will maintain an ISMS in accordance with ISO 27001, ensuring:

(a) Risk assessment and treatment methodologies for data security, identifying and mitigating potential security threats;

(b) Continuous monitoring and improvement of security controls, including the adoption of emerging security technologies;

(c) Clear documentation and communication of security policies, ensuring all personnel are aware of their responsibilities;

(d) Incident management and response procedures, with dedicated teams to investigate, contain, and resolve security incidents effectively; and

(e) Implementation of robust logging and monitoring mechanisms to detect and respond to anomalies in real time.

4 Secure Data Handling

All personnel must adhere to secure data processing standards, including:

(a) Access control mechanisms to limit unauthorized data access, ensuring only those with a legitimate need can access sensitive information;

(b) Data classification and encryption protocols for sensitive information, providing an additional layer of protection;

(c) Secure storage and transmission measures, including end-to-end encryption and secure data exchange platforms where appropriate;

(d) Regular security awareness training and compliance programs, ensuring employees remain vigilant and informed about the latest threats and best practices; and

(e) Implementation of secure coding practices in software development to prevent vulnerabilities such as SQL injection and cross-site scripting.

5 Access Control and Authentication

All personnel must adhere to access control and authentication standards, including:

(a) Role-based access control (RBAC) must be enforced to ensure that access privileges are granted based on job responsibilities;

(b) Multi-factor authentication (MFA) is required for all critical systems to prevent unauthorized access;

(c) Periodic access reviews must be conducted to ensure appropriate privileges and revoke access for former employees or role changes; and

(d) Secure password policies must be enforced, including minimum complexity requirements.

6 Risk Management and Compliance

Imricor will manage risk and compliance through several methods, including:

(a) Regular risk assessments must be performed to identify vulnerabilities, classify risks, and implement necessary mitigation strategies;

(b) Compliance with legal, regulatory, and contractual obligations is mandatory to ensure adherence to industry standards;

(c) Security audits and penetration testing must be conducted periodically to evaluate the effectiveness of security controls; and

(d) Threat intelligence and security research must be continuously monitored to anticipate and counter emerging threats.

7 Incident Response and Business Continuity

Imricor will ensure timely and effective response to incidents ensuring business continuity, including:

(a) A documented incident response plan must be in place, outlining procedures for identifying, containing, and resolving security incidents;

(b) All security incidents must be reported and investigated promptly to minimize damage and prevent recurrence;

(c) Business continuity and disaster recovery plans must be tested periodically to ensure resilience against cyber-attacks and other disruptive events; and

(d) Secure backup procedures must be in place, ensuring that critical data can be recovered in case of system failure or data corruption.

8 Data Retention and Disposal

Imricor will maintain policies and procedures for data retention and disposal, including:

(a) Data retention policies must be defined based on regulatory and business requirements, ensuring data is stored only for the necessary duration;

(b) Secure disposal methods, including data wiping and destruction, must be followed to prevent unauthorized access to obsolete information; and

(c) Access logs and audit trails must be maintained to ensure compliance with retention policies and track data access activities.

9 Third-Party Security Management

Third-party security management procedures will include:

(a) All third-party service providers must adhere to equivalent security standards, ensuring that external partners align with Imricor's security requirements.

(b) Security agreements must be included in contracts with external vendors where appropriate, clearly defining expectations, responsibilities, and compliance obligations;

(c) Third-party risk assessments must be conducted regularly to evaluate potential security risks associated with external partnerships; and

(d) Data-sharing agreements must be implemented to specify secure transmission methods and handling procedures for shared information.

10 Continuous Improvement

Imricor is committed to continuous improvement, including:

(a) Regular reviews and updates to security policies and controls must be conducted to ensure compliance with evolving security threats;

(b) Feedback mechanisms must be established to enhance security practices, including employee suggestions and security incident lessons learned;

(c) Security awareness campaigns must be launched periodically to reinforce the importance of cybersecurity among employees; and

(d) Investment in advanced security technologies and infrastructure must be prioritized to strengthen defenses against sophisticated threats;

11 Enforcement

Non-compliance with this policy may result in disciplinary action, including termination and legal consequences. Violations of security policies may also lead to reputational damage, regulatory penalties, and financial losses for Imricor. Employees, contractors, and third parties are expected to adhere strictly to this policy and report any suspected security breaches immediately.

11 Review of this Secure Data Processing policy

This policy may be amended by the Board of Directors from time to time, to align with evolving security standards, business needs, and regulatory changes.

Approved by the Board of Directors of Imricor Medical Systems, Inc.