Adaptix Medical Device Security Policy

Medical device security (top-level)

a) Adaptix has established and shall maintain this Medical Device Security Policy to:

- protect medical device associated information assets and supporting infrastructure from potential internal and external threats and hazards,
- protect against reasonably anticipated unauthorised disclosures and uses of the medical device's sensitive information (e.g., patient health information, customer information, intellectual property),
- protect against reasonably anticipated internal and external threats and hazards that may result in an impact to patient and user of the medical device safety, and
- maintain the confidentiality, integrity and availability of sensitive information stored, handled, or transmitted by the medical device.

b) Adaptix shall establish, document, distribute, and periodically review/update the Medical Device Security Policy and associated standards, and procedures to support maturity development and comply with applicable laws, statutory, regulatory, or contractual obligations, industry leading practices, organisational policies, and audit procedures.

c) Adaptix shall implement medical device security roles, responsibilities, resources, tools, technologies, and processes needed for the successful implementation of this medical device security policy.

d) Company management, along with the Security Risk Management Team shall be responsible for coordinating, developing, implementing, and maintaining the medical device security program that implements this policy.

e) The Medical Device Security Policy shall be approved by company management, maintained, and made available by management in accordance with business requirements and relevant laws and regulations.

f) Procedures will be established to review the Medical Device Security Policy at least annually, update it as needed, and make it available to all colleagues and individuals working on behalf of the organisation.

g) Ad-hoc, supplemental medical device security requirements/guidance will be developed, approved, and communicated, as needed, between regular policy review/update cycles.

Adaptix Medical Device Security Policy
(Rev B)

Medical device security operations

a) Adaptix shall develop and implement a security risk management process that:

- identifies medical device security requirements to be built into the design of new devices,
- protects against all reasonably anticipated threats or hazards to the confidentiality, integrity, and availability of the medical device and sensitive information, and
- manages security risk assessments and technical security testing, mitigation, acceptance, and reporting, and
- controls security risks in third-party components.

b) Adaptix shall develop and implement a threat event and incident handling process that:

- monitors industry sources for threat events, including third-party components, and incidents and has processes in place to triage security.

c) Adaptix shall develop and implement a security education and training process that:

- establishes and maintains a medical device security awareness program that communicates security requirements, industry trends, and other security-related topics to personnel responsible for managing the security of the organisation's medical devices,
- ensures that security personnel and individuals working on behalf of the organisation are informed of their responsibilities to protect the confidentiality, integrity, and availability of medical devices and sensitive information,
- directs that security personnel and individuals working on behalf of the organisation complete training within 90 days of hire and at least annually after hire, and
- ensures that supplemental role-based training be provided to security personnel and individuals working on behalf of the organisation who have a specific business need or whose duties involve designing, developing, or maintaining the organisation's medical devices.

Supporting security controls and implementation (by organisational function)

a) Human Resources shall

- work with the appropriate organisation offices to establish controls that ensure security personnel and individuals working on behalf of the organisation are suitable for the roles for which they are placed and are trained on their information security responsibilities,

- work within the organisation to, define, document, and enforce security roles and responsibilities of security personnel and individuals working on behalf of the organisation, and

- establish, document, review/update, and enforce a formal disciplinary process for colleagues and individuals working on behalf of the organisation who have violated information security policies and procedures.

b) Contracting and Outsourcing shall

- protect medical devices and information that is generated, accessed, stored, transmitted, processed, or otherwise handled by external third parties,

- establish and maintain a formal process for engaging and assessing the security practices (i.e., vendor risk) and security design and implementation (i.e., device risk) that is associated with third parties who provide services and or medical devices that the organisation procures; this shall be included in the Vendor Approval Form process where applicable, and shall be included in applicable financial, Quality and legal diligence checks when entering into a contract (See next point)

- require contractual obligations for reporting and mitigating security vulnerabilities in products (e.g., software) or services, and

- terminate business with external third parties who collect, access, store, transmit, process or otherwise handle organisation medical devices and information unless:

    - the third-party security requirements are reviewed and approved by security staff, or
    - a contract is in place stating that the third party has implemented all appropriate administrative, physical, and technical safeguards.

c) Quality & Regulatory Affairs shall

- ensure that the design, operation, use, and management of medical devices adheres to applicable laws, statutory, regulatory or contractual obligations, and information security requirements,

- establish and maintain a policy, standards, procedures, and guidance to ensure compliance with applicable laws, statutory, regulatory or contractual obligations, industry leading practices, and audit procedures,

- establish processes to address failure to comply with the Medical Device Security Policy and subsequent standards which can result in disciplinary actions up to and including termination of employment for colleagues or terminations of contracts for contractors, partners, consultants, and other entities, and

- verify that technical security requirements, appropriate to the nature of the device level or hazard and security risk, have been established.

d) Servicing and Production shall

- establish and maintain a program to track medical device sold or leased to Health Delivery Organisations (HDOs),
- monitor the state of deployed devices through remote services where feasible,
- ensure that technical security requirements are enforced.

e) Business Systems and Engineering shall

- protect the confidentiality, integrity, and availability of the organisation's processes, intellectual property, and other resources used to create and manufacture medical device,
- establish, maintain, document and review/update sufficient controls to restrict physical and logical access to sensitive information based on a need to know or least privilege basis (i.e., role-based access), and
- implement physical, technical, and administrative safeguards to protect all forms of electronic media (e.g., laptops, CD-ROMs, USB drives, disks, tapes) containing sensitive information (e.g., patient data) from unauthorised access.
- ensure that strategies and plans are in place to counteract interruptions to device operations and to protect critical device operational processes from the effects of major failures of system components or disasters and to ensure their timely resumption, and
- establish and maintain a business continuity program to quickly resume device operational activities and recover information in the event of system failure or other disaster.

f) Systems and Software Engineering shall

- establish and maintain a secure life-cycle design program that incorporates security into the device at the initial design and requirements stage,
- assign responsibilities for monitoring threat and vulnerability information, and
- conduct risk assessments for legacy devices not beyond EOS (End of Support) and implement extra security controls (e.g., segmentation) for devices that have reached EOGS (End of Guaranteed Support) and are no longer supported.

g) Senior Leadership Team

- The Adaptix Senior Leadership Team will meet once a month and cover any security matters from a strategic and tactical point of view, reviewing all considerations from Cyber Security Post Market Surveillance Plan and activities. In addition, the CEO and COO will always be ready as part of the required responsible owners of security incidents once they have escalated past a certain threat level in accordance with the Security Incident Handling and Response Plan.