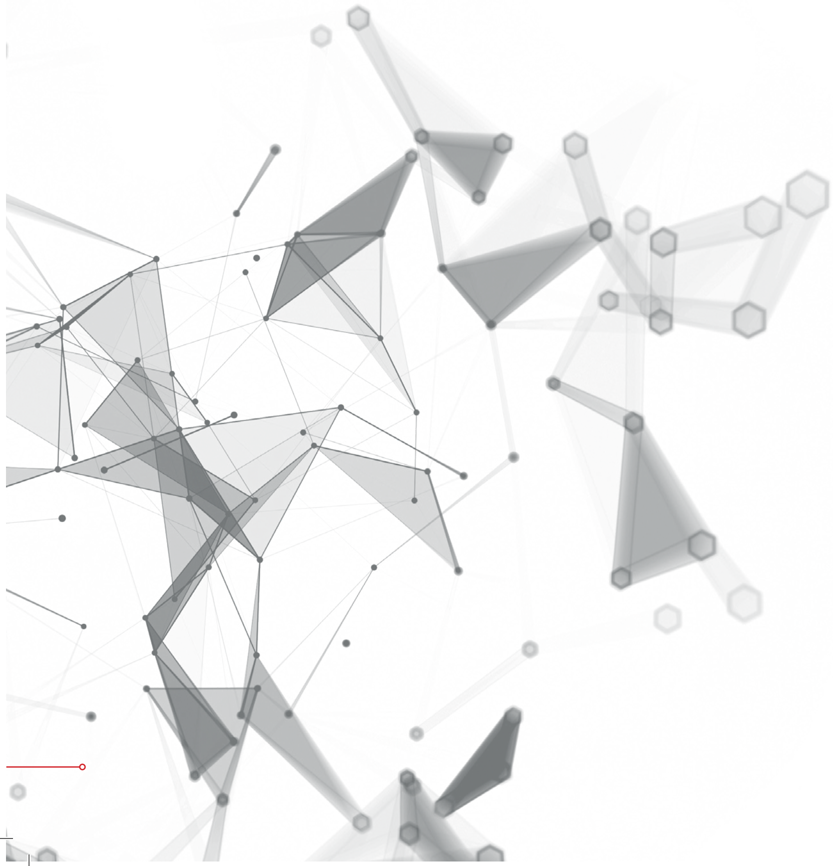
حكومة دبي
GOVERNMENT OF DUBAI

مركز دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER

ELECTRONIC BIOMEDICAL DEVICES (EBMD) SECURITY STANDARD

VERSION 1.0



Electronic Biomedical Devices (EBMD) Security Standard

VERSION 1.0

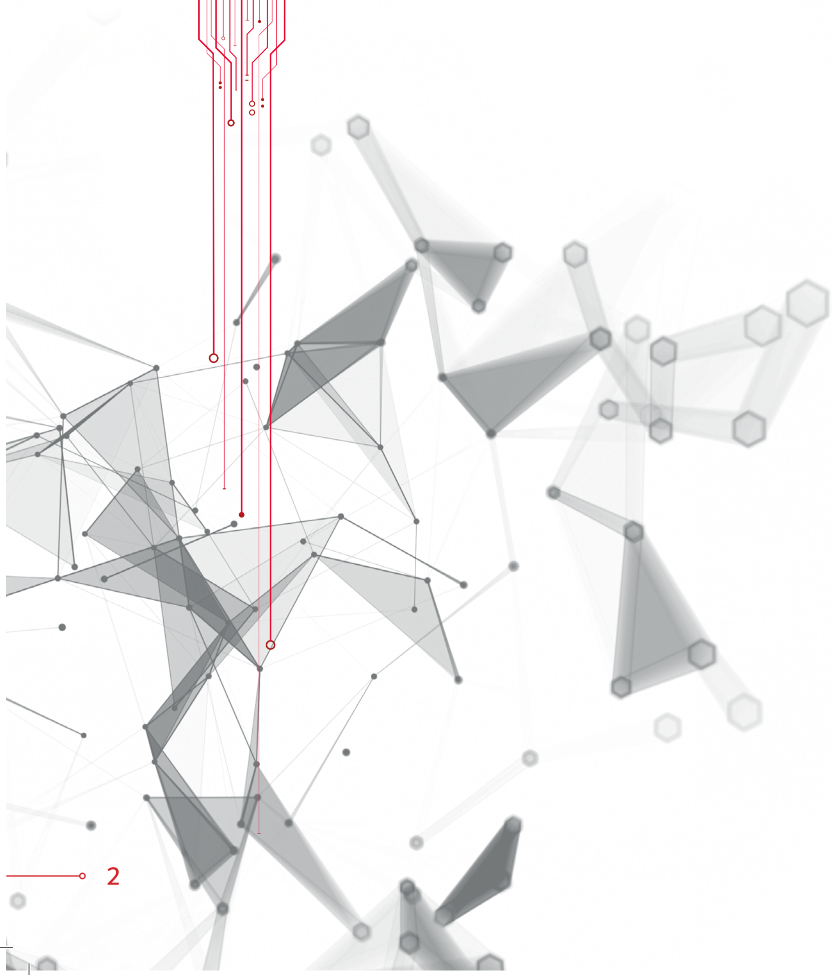
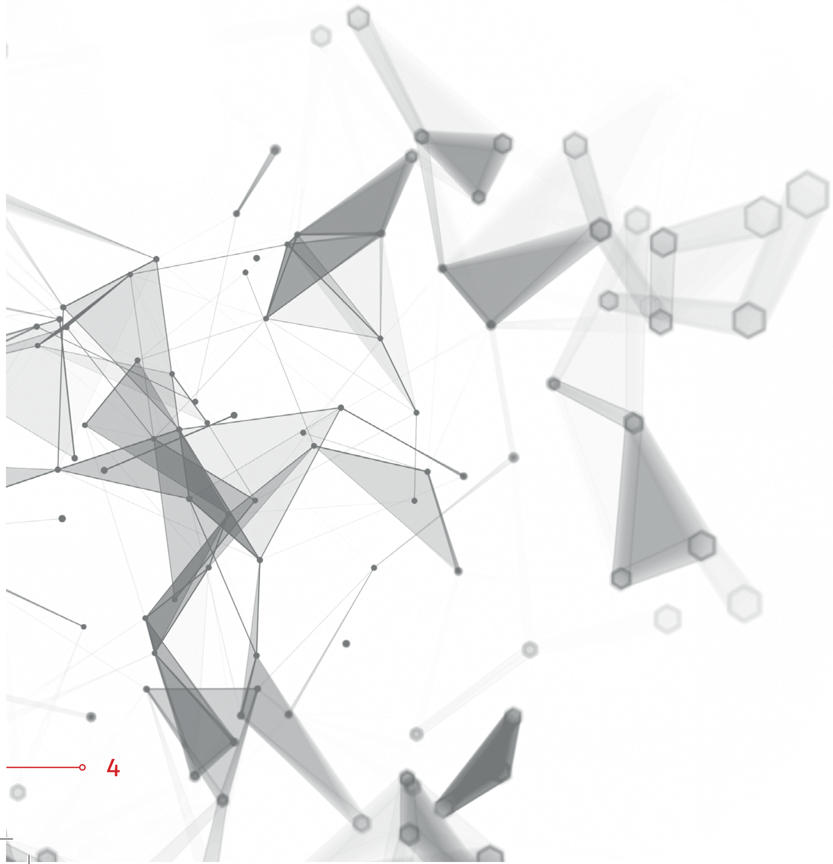


TABLE OF CONTENTS



INTRODUCTION

Biomedical Devices (BMD) are using more and more electronic means for functioning, processing and communicating. This provides many chances for medical progress, but also entails risks related to ICT security. Therefore, the Dubai Electronic Security Centre (DESC) has developed this standard for ensuring the secure operation of electronic biomedical devices in Dubai.

This standard is largely based on the IoT Security Standard (see also www.desc.ae/standards), which also has been produced by DESC. It covers all electronic biomedical devices. Any other biomedical devices, such as bandages, plaster, etc., are not addressed by this standard. For them, the already existing regulations apply.

There are several interest groups that have done work on the security of biomedical devices. The work that was considered when developing this standard includes:

- Australian Regulatory Guidelines for Medical Devices, Section 4. Classification of medical devices, Version 1.1. 2011
- European Union MEDICAL DEVICES Guidance Document – Classification of medical devices, June 2010
- Medicines (Database of Medical Devices) Regulations 2003, New Zealand
- Title 21 of the Code of Federal Regulations (CFR), Parts 862-892 – Classification in US, approved by FDA
- Schedule 1, Part 1 of the Canadian Medical Devices Regulations (CMDR) SOR/98-282

Additionally, the following documents are indispensable for the use of this standard:

- ISO/IEC 27001:2013 – Information Technology – Information security management system – Requirements
- Information Security Regulation ISR V2.0 – DESC
- IoT Security Standard – DESC, amended to address biomedical devices, attached to this document
- HIPAA (Health Insurance Portability and Accountability Act) – 1996

ACKNOWLEDGEMENT

DESC acknowledges the extremely valuable contribution that Dubai Health Authority (DHA) made to this standard; DHA's profound medical expertise and their excellent understanding of the procedures related to BMDs helped to make this standard complete.

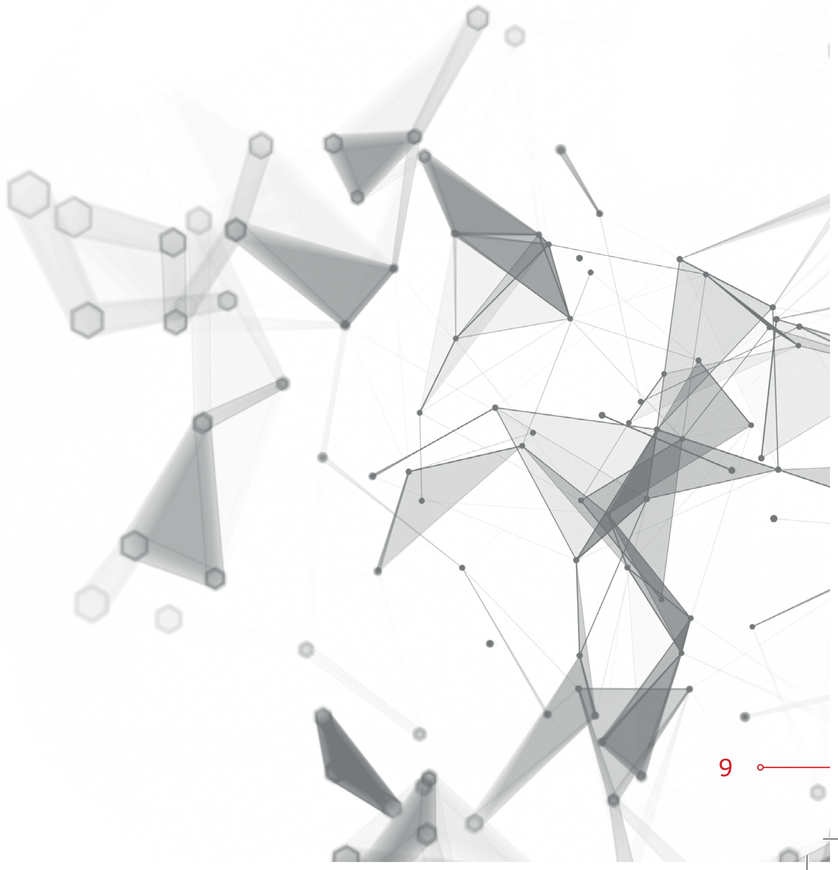
1 SCOPE

1 SCOPE

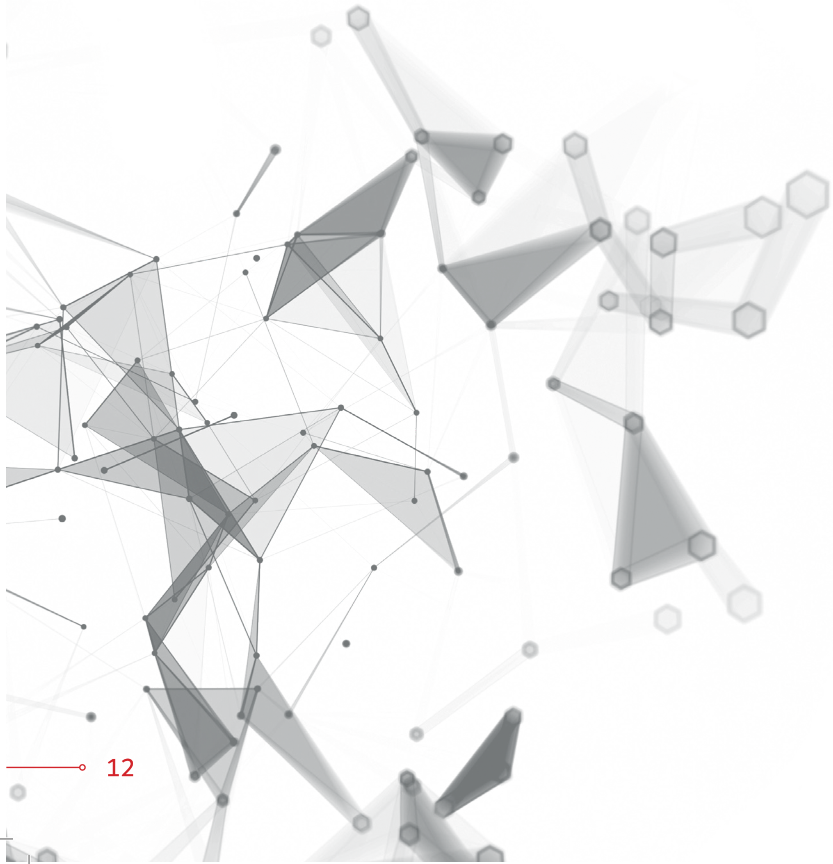
This Standard provides mandatory and recommended controls for the security of electronic biomedical devices (EBMD). The standard is applicable to all manufacturers of biomedical devices in the scope of this standard, wishing to offer their products and/or services in Dubai, and to all hospitals in Dubai wishing to use such biomedical devices.

This standard can be used by DHA to license biomedical devices.

Any non-electronic biomedical devices are not within the scope of this standard.



2 STRUCTURE OF THIS STANDARD



2 STRUCTURE OF THIS STANDARD

This clause describes the structure of this standard, and its relation to the already existing IoT Security Standard.

This structure of this standard is:

1. Classification of EBMDs (Section 3)

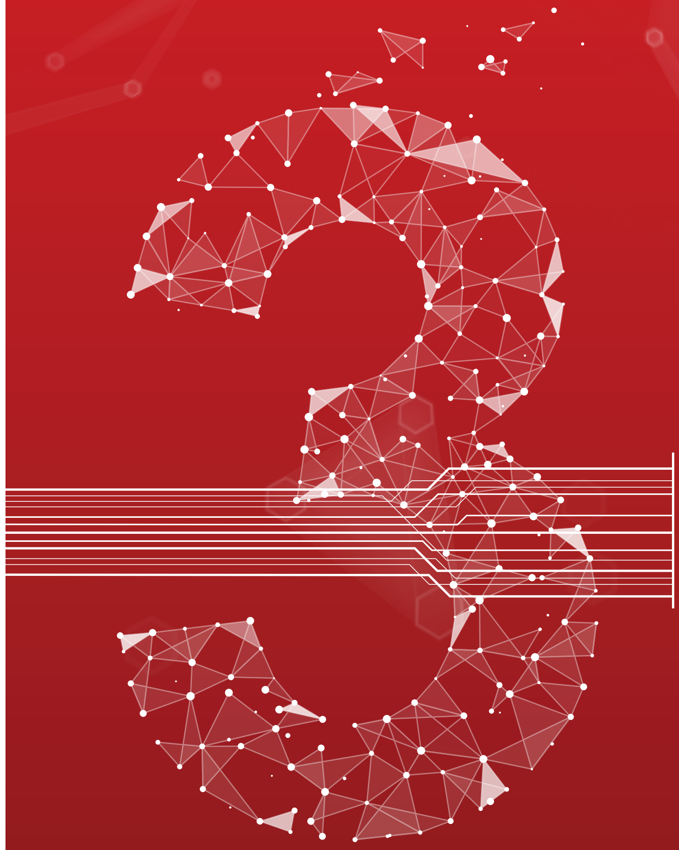
   Biomedical devices, even if restricted to those that are electronic devices, are extremely diverse. In order to understand the risk scenarios involved with the use of EBMDs, it is helpful to apply a classification, based on the amount of risks that are involved, and the controls needed to protect against such risks. Other regions and countries, such as EU, US, Canada and Australia, have already introduced classifications (see also Annex B). The classification applied for this standard is described in Section 3.

2. Application of EBMD Security Controls based on classification (Section 4).

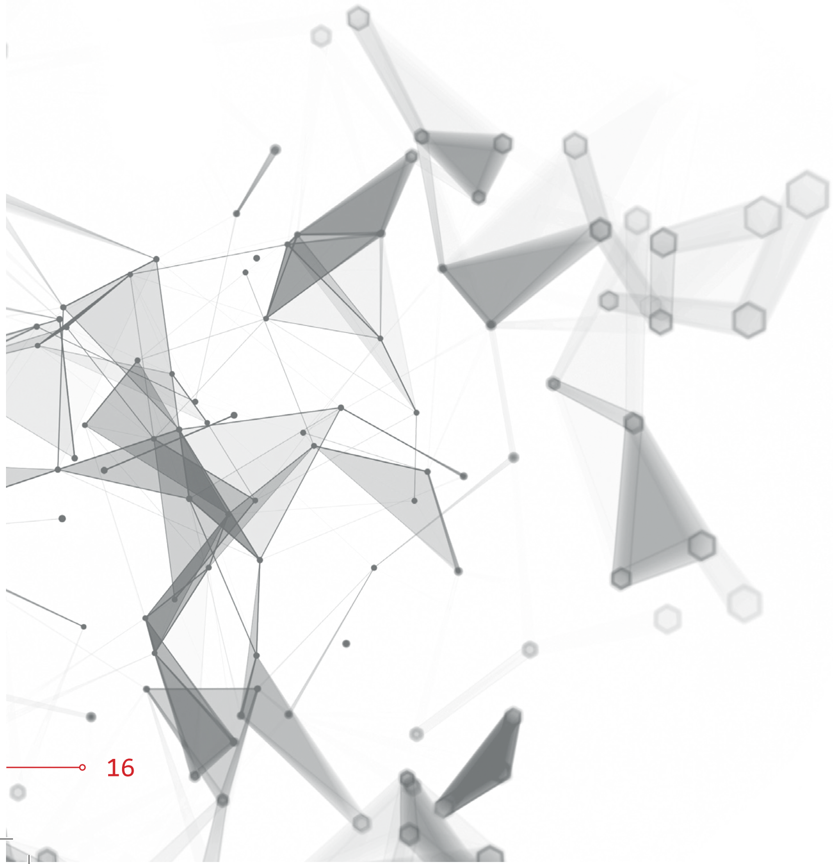
   Based on the classification of a particular biomedical device, controls from the IoT security standard (see Annex A) apply. Please note that the IoT Security Standard has been amended to contain only controls applicable for biomedical devices. Section 4 also explains which controls apply for the various classification levels.

3. Additional Electronic Biomedical Security Controls (Section 5)

   As electronic biomedical devices fulfil specific functions, there are additional controls that shall be applied for those devices, in direct relation to their medical function. These controls are contained in Section 5 of this standard.



3 CLASSIFICATION OF ELECTRONIC BIOMEDICAL DEVICES



3 CLASSIFICATION OF ELECTRONIC BIOMEDICAL DEVICES

3.1 Classification of Electronic Biomedical Devices for Dubai

The classification labels and details that have been chosen for this standard makes use of the concepts described in

- Australian Regulatory Guidelines for Medical Devices, Section 4. Classification of medical devices, Version 1.1. 2011
- European Union MEDICAL DEVICES Guidance Document – Classification of medical devices, June 2010

An overview of international classification rules can be found in Annex C.

The levels used for this classification are oriented on the potential negative impact a problematic EBMD might have on the patient, therefore some detailed distinctions have been made:

Classification	Level of Impact
Class I	Low
Class I – sterile (see 3.2) Class I – measuring function (see 3.2) Class II a	Low-Medium
Class II b	Medium – High
Class III	High
Active implantable medical devices (AIMD)	High

The manufacturer is responsible for determining the classification of a device using a set of classification rules based on the:

- manufacturer's intended use of the device
- level of impact to patients, users and other persons
- degree of invasiveness in the human body
- duration of use

Identical devices may be classified differently if they are to be used in different parts of the body. This is why the manufacturer's intended use of the device is so critical to determining the appropriate classification. The intended use should be clarified in the report card.

In DHA, there are also two other classification models, namely:

EQUIPMENT FUNCTION

Includes various areas in which therapeutic, diagnostic, analytical and miscellaneous equipment is used.

Category	Function Description	Point Score
Therapeutic	Life Support	10
	Surgical and intensive care	9
	Physical therapy and treatment	8
Diagnostic	Surgical and intensive care monitoring	7
	Additional physiological monitoring and diagnostic	6
Analytical	Analytical laboratory	5
	Laboratory accessories	4
	Computers and related	3
Miscellaneous	Patient related and other	2

PHYSICAL RISK ASSOCIATED WITH CLINICAL APPLICATION

Lists the potential patient or equipment risk during use.

Physical Risk	Point score
Potential patient death	5
Potential patient or operator injury	4
Inappropriate therapy or misdiagnosis	3
Equipment damage	2
No significant identified risk	1

These different classifications can be brought together in the following simple alignment (in case where the Equipment Function Classification and the Physical Risk Classification do not lead to the same result in matching this standard's classification, the maximum should be used):

This Standard's Classification	Equipment Function Classification (b)	Physical Risk Classification (c)
Class III or Active implantable medical devices - High	10 - Life Support 9 - Surgical and intensive care	5 - Potential patient death
Class II b – Medium - High	8 - Physical therapy and treatment 7 - Surgical and intensive care monitoring	4 - Potential patient or operator injury
Class II a - Medium	6 - Additional physiological monitoring and diagnostic 5 - Analytical laboratory	3 - Inappropriate therapy or misdiagnosis
Class I – Sterile or with measuring function	4 – Laboratory accessories 3 – Computers and related	2 - Equipment damage
Class I - Low	2 - Patient related and other	1 – No significant risk

Examples:

- Equipment Function Classification = 7 and Physical Risk Classification = 4 ▯ Class II b – Medium – High in this standard

- Equipment Function Classification = 4 and Physical Risk Classification = 5 ▯ Class III or Active implantable medical devices - High in this standard

3.2 Classification Principles

- Maximum Principles
  - If more than one classification rule applies, always the rule leading to the highest classification should be chosen.
  - If an EBMD is used in combination with other EBMDs, each EBMD should be classified individually.
  - For systems and procedure packs, the classification for the entire system or pack is the highest classification of any individual EBMD in the system or pack.
- Devices with a measuring function

An EBMD is considered to have a measuring function if the device is intended by the manufacturer to measure:

- Quantitatively a physiological or anatomical parameter;
- A quantity or a qualifiable characteristic of energy or of substances delivered to or removed from the human body.

The measurements given by a medical device should:

- Display in UAE legal units of measurement, and
- Be accurate to enable the device to achieve its intended purpose.

Manufacturers of Class I EBMDs that have a measuring function should classify this device in the “Low – Medium” impact classification.

- EBMDs required to be sterile

Some medical devices are required to be sterile when used to minimize the risk of infection. Such medical devices should be terminally sterilized to a Sterility Assurance Level (SAL) of at least 10-6, unless this is not possible due to device material incompatibility with the proposed sterilization process. It is the responsibility of the manufacturer to determine the most appropriate method for achieving the required SAL for a particular device after due consideration of the design and construction of the device.

Devices that are required to be sterile, but cannot be subjected to terminal sterilization, can be manufactured aseptically, for example by sterile filtration. Devices manufactured in this manner have a lower SAL than those subjected to terminal sterilization.

Manufacturers of Class I EBMDs that have to be sterile should classify this device in the “Low – Medium” impact classification.

- Duration

When determining the appropriate classification for an EBMD, the manufacturer should take the account of the duration of its use, distinguishing:

Period of intended use	Descriptive label
Less than 60 minutes	Transient
At least 60 minutes, but no more than 30 days	Short term
More than 30 days	Long term

3.3 Classification Decision Tree

Manufacturers should use the decision tree below to identify the appropriate classification for their EBMD. All classification rules should be considered to avoid important aspects being overlooked.

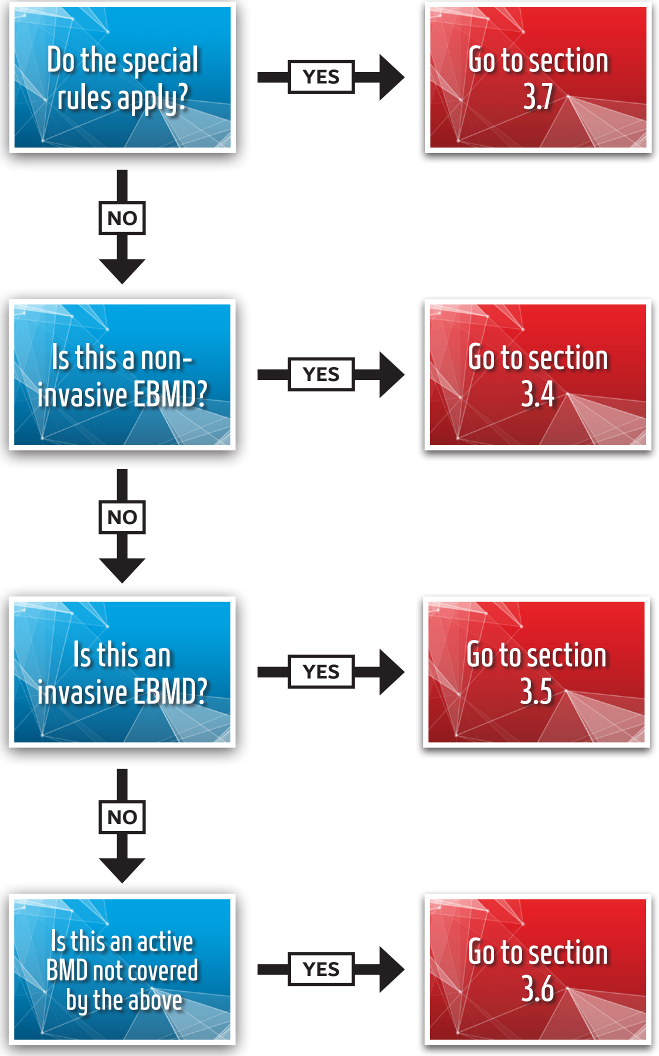

Do the special rules apply?
YES
Go to section 3.7
NO
Is this a non-invasive EBMD?
YES
Go to section 3.4
NO
Is this an invasive EBMD?
YES
Go to section 3.5
NO
Is this an active BMD not covered by the above
YES
Go to section 3.6

Figure 1 Classification decision tree

3.4 Non-Invasive EBMDs

Rule 1 A non-invasive EBMD is Class I, unless the device is classified at a higher level under another rule in this clause.

Rule 2a A non-invasive device to modify the biological or chemical composition of blood, other body liquids, or other liquids to be infused in the patient is classified as Class IIb.

Rule 2b A non-invasive device to be used in treatment consisting of filtration, centrifugation or exchanges of gas or heat is classified as Class IIa.

3.5 Invasive EBMDs

› Transient use

Rule 1a Surgically invasive EBMDs for transient use to diagnose, monitor, control or correct a defect of the heart, or central circulatory system through direct contact are classified as Class III.

Rule 1b A surgically invasive EBMD for transient use to supply ionizing radiation is Class IIb.

Rule 1c A surgically invasive EBMD for transient use to have a biological effect is Class IIb.

Rule 1d A surgically invasive EBMD for transient use to administer medicine via a delivery system, and where the administration is potentially hazardous to the patient is Class IIb.

› Short term use

Rule 2a A surgically invasive EBMD for short-term use to supply ionizing radiation is Class IIb.

Rule 2b A surgically invasive EBMD for short-term use to be specifically used to diagnose, monitor, control or correct a defect of the heart, or central circulatory system, through direct contact with these parts of the body is Class III.

Rule 2c A surgically invasive EBMD for short-term use to be used in direct contact with the central nervous system is Class III.

- Long term use

Rule 3a Invasive EBMDs that are for long-term use are classified as Class IIb.

Rule 3b A surgically invasive EBMD for long-term use to be used in direct contact with the heart, the central circulatory system or the central nervous system is Class III.

Rule 3c A surgically invasive EBMD for long-term use intended by the manufacturer to have a biological effect is Class III.

Rule 3d A surgically invasive EBMD for long-term use to administer medicine is Class III.

3.6 Active EBMDs

Rule 1 An active EBMD is Class I, unless the device is classified at a higher level under another rule in this clause.

- Therapeutic use

Rule 2a An active EBMD for therapy to administer energy to a patient, or exchange energy to or from a patient is Class IIa.

Rule 2b An active EBMD to administer or exchange energy in a potentially hazardous way, having regard to the nature, density and site of application of the energy is Class IIb.

Rule 2c An active EBMD to control or monitor, or directly influence the performance of an active medical device for therapy of the kind in the previous entry is Class IIb.

- Diagnostic use

Rule 3a An EBMD to supply energy that will be absorbed by a patient's body (except a device that illuminates the patient's body in the visible spectrum) is Class IIa.

Rule 3b An EBMD to be used to image in vivo distribution of radiopharmaceuticals in patients is Class IIa.

Rule 3c An EBMD used for direct diagnosis or monitoring of vital physiological processes of a patient, excluding devices mentioned in the previous entry is Class IIa.

Rule 3d An EBMD to monitor vital physiological parameters of a patient, and the nature of variations monitored could result in immediate danger to the patient is Class IIb.

Rule 3e An EBMD to emit ionizing radiation and to be used for diagnostic or therapeutic interventional radiology is Class IIb.

Rule 3f An EBMD to control, monitor or directly influence the performance of a device in the previous entry is Class IIb.

- Administrative use

Rule 4a An active EBMD to administer or remove medicine, body liquids or other substances is Class IIa.

Rule 4b An active EBMD to administer or remove medicine, body liquids or other substances in a way that is potentially hazardous to the patient, having regard to the substances, the part of the body concerned, and the characteristics of the device is Class IIb.

3.7 Special Rules

- Recording X-Ray diagnostics

Rule 1 A non-active EBMD to record x-ray diagnostic images such as x-ray films, photostimulable phosphor plates is Class IIa.

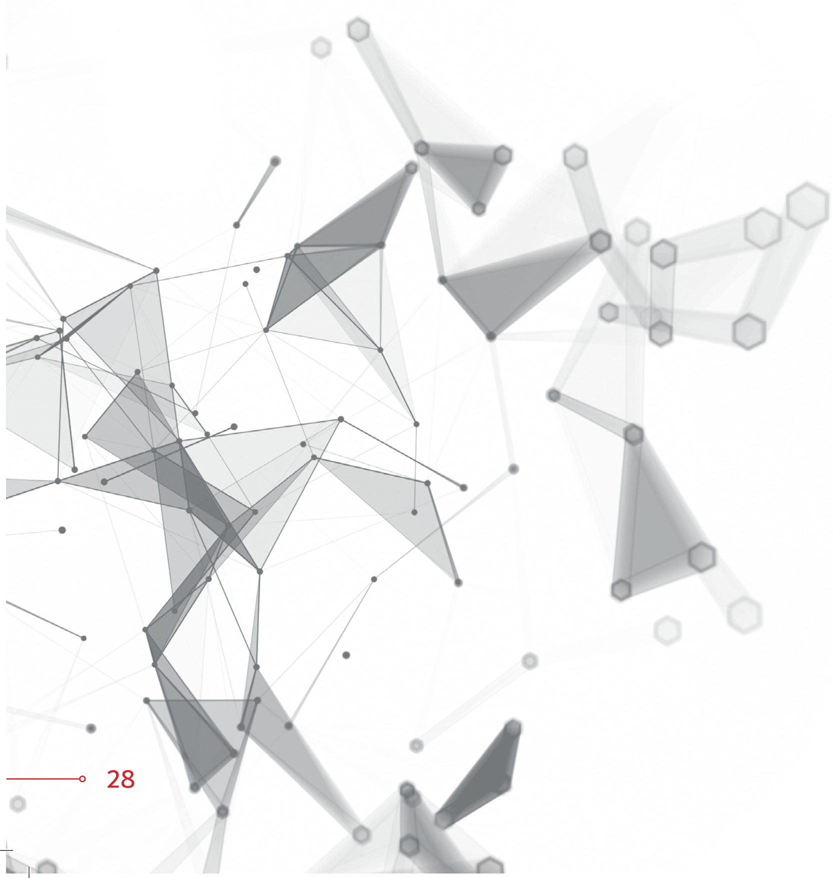
- Active Implantable EBMDs

Rule 2a An active implantable EBMD is classified as Class AIMD.

Rule 2b An implantable accessory to an active implantable EBMD is Class III.

Rule 2c An active EBMD to control, monitor or directly influence the performance of an active implantable medical device is Class III.

4 APPLICATION OF EBMD SECURITY CONTROLS



4 APPLICATION OF EBMD SECURITY CONTROLS BASED ON CLASSIFICATION

4.1 Overview

Which controls are applied for the different classification levels is depicted in the figure below:

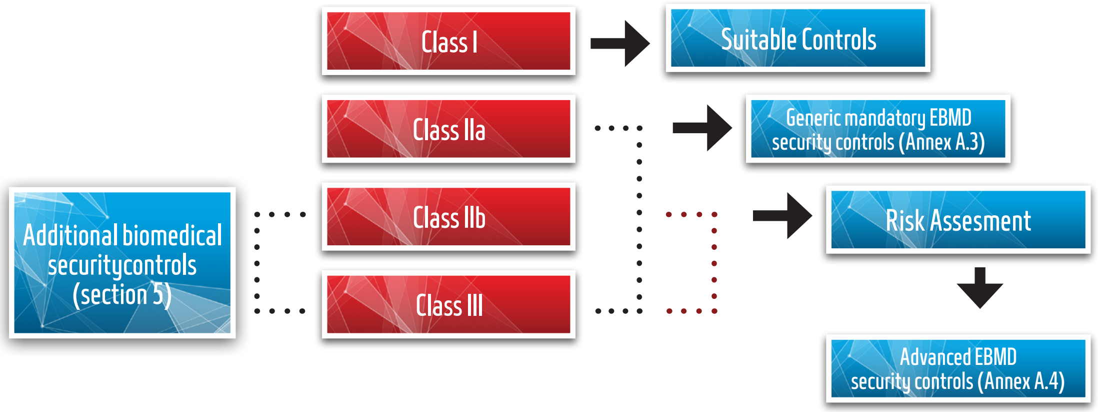

Class I
Suitable Controls
Class IIa
Generic mandatory EBMD security controls (Annex A.3)
Additional biomedical securitycontrols (section 5)
Class IIb
Risk Assesment
Class III
Advanced EBMD security controls (Annex A.4)

Figure 2 Application of EBMD security controls based on classification

4.2 EBMD Security Controls for Class I

As EBMDs of Class I are not very critical, it is sufficient for these EBMDs to apply those security controls that have been determined based on the information security risk assessment (which might be carried out as part of the ISO/IEC 27001 or ISR implementation). Controls cited in this standard do not need to be applied.

4.3 EBMD Security Controls for Class II a

All controls from section A.3 of this standard apply.

In addition, hospitals and other organizations using biomedical devices, should be encouraged to achieve ISO/IEC 27001 and/or ISR certification.

4.4 EBMD Security Controls for Class II b and Class III

All controls from Section A.3 of this standard apply.

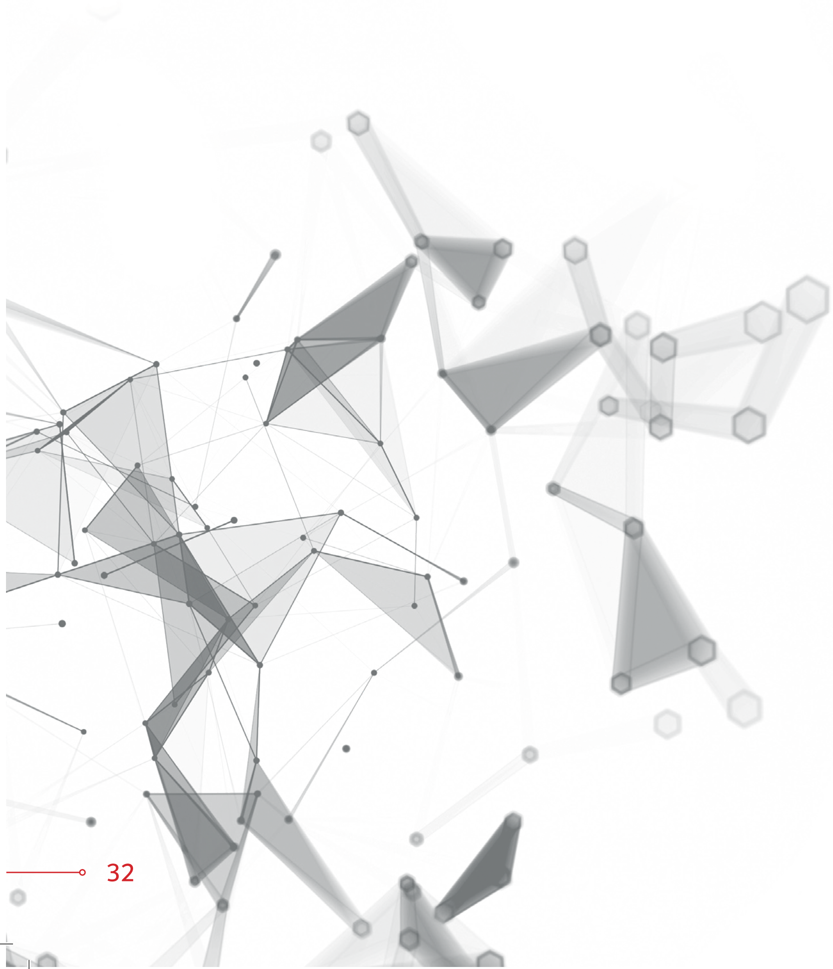
In addition, hospitals and other organizations using biomedical devices, should be encouraged to achieve ISO/IEC 27001 and/or ISR certification.

Controls from Section A.4 should be applied on a risk basis.

All controls from Section 5 of this standard apply.

DUBAI ELECTRONIC SECURITY CENTER
مركز دبي للأمن الإلكتروني

5 ADDITIONAL EBMD SECURITY CONTROLS



5 ADDITIONAL ELECTRONIC BIOMEDICAL SECURITY CONTROLS

The following security controls are mandatory for all electronic biomedical devices of Class IIb and III and are to be applied in addition to the controls from Annex A. Each control includes a mandatory part the manufacturer has to adhere to, and an optional part, which can be chosen from, based on the risk assessment.

5.1 Report Card (MDS2)

MANDATORY

1 A Manufacturer Disclosure Statement for Medical Device Security – MDS2 shall be provided for each device.

2 All details in the MDS2 shall be updated as per the Annual Maintenance Contract (AMC).

3 The procurement process shall ensure that manufacturers provide the following information related to the security of their EBMD:

- The intended use of the device.
- Risk assessment report and controls put in place to protect the EBMD, including:
    - A specific list of all security risks that were considered in the design of the EBMD.
    - A statement about who conducted the risk assessment, and who approved it.
    - A statement about technical security testing that was conducted, by whom, and what the results were.
    - A specific list and justification for all security controls that were established for your device, and a justification for all controls from this standard that were omitted.
    - A traceability matrix that links the security controls to the risks that were considered.
- A summary describing the plan for providing validated software updates and patches as needed throughout the lifecycle of the medical device to

continue to assure its safety and effectiveness.

- An indication whether the EBMD will be remotely accessed, and if so, which controls are in place to secure that access.
- A summary describing controls that are in place to assure that the EBMD software will maintain its integrity (e.g. remain free of malware) from the point of origin to the point at which that device leaves the control of the manufacturer.
- Device instructions for use and product specifications related to recommended security controls appropriate for the intended use environment (for example, anti-virus software or use of firewall).

5.2 Secure Remote Access

MANDATORY

A manufacturer of an EBMD device should:

1. In order to remotely access an EBMD after selling, obtain consent for such access from the provider of the device. An agreement between manufacturer and provider can be used to specify the type, frequency, etc. of such access. Consent of the patient may be obtained through the provider notifying the patient of such agreement.

2. Notify the provider when accessing the device remotely, including the name of the person with such access, the kinds of tasks that can be performed through such access, and the software used to access the device. Such notification can be in the form of an audit log (see 3.).

3. Maintain an audit log for each time of remote access and make such log accessible to the provider.

When a supplier accesses a machine related to EBDMs for maintenance, this can only happen after IT approval of the access.

OPTIONAL

1. Implement multi-factor authentication for accessing the device.

2. Secure data in motion and data at rest using encryption.

3. Install automated tools to track access, or identify attempts at unauthorized access, to the device.

4. Adopt whitelisting approaches and changeable passwords for accessing the device.

5.3 End of life of the Device

MANDATORY

Not later than 90 days after a manufacturer declares that it will no longer sell an EBMD, the manufacturer of the device should:

1. Provide any provider of the device with the report card (see 5.4.2 and 5.4.3 above).

2. To the extent practicable, inform any provider of the device that the device will no longer be manufactured.

3. Provide notice to any provider of the device of the date on which the last cybersecurity fix or update will be provided;

4. Notify DHA of such declaration.

5. Provide any provider of the device with the following information related to the device:

   - Compensating controls on how to securely configure the EBMD if the device stays in operation past the date on which the manufacturer stops providing cybersecurity fixes or updates.
   - Documentation on secure preparation for recycling and disposal of the device.
   - Specific guidance regarding supporting infrastructure architecture, including network segmentation and device isolation requirements.
   - Instructions on how to delete any personally identifiable information, protected health information, or other site-specific sensitive data such as configuration files.

A data wiping process should be in place for all EBMD devices at their end of life, and it should be ensured that this is conducted as outlined in the process.

5.4 Procurement Security

MANDATORY

The procurement process should ensure that manufacturers did establish a set of controls to create security for the EBMD they are producing. It should further ensure that manufacturers did conduct a risk assessment (this can be part of the ISO/IEC 27001 or ISR V2 risk assessment), which addressed:

- Identification of assets, threats, and vulnerabilities;
- Assessment of the impact of threats and vulnerabilities on device function-

ality and patients;

- Assessment of the likelihood of a threat and of a vulnerability being exploited;
- Determination of risk levels and suitable mitigation strategies;
- Assessment of residual risk and risk acceptance criteria.

The procurement process should also ensure that the risk assessment did include vulnerability assessment and software validation.

The procurement process should further ensure that manufacturers did carefully consider the balance between security controls and the usability of the EBMD in its intended environment of use (e.g. home use vs. health care facility use) to ensure that the security controls are appropriate for the intended users. For example, security controls should not unreasonably hinder access to a device intended to be used during an emergency situation.

A justification for the security functions chosen in EBMDs (this can, for example, be done in the report card) should be included.

Please note: The above controls can also be addressed by ensuring that the device is FDA and/or CE approved.

OPTIONAL
In addition to the controls listed in Section 5 of this standard, the following are examples of security controls that can be considered in the procurement process:

- Use automatic timed methods to terminate sessions within the system where appropriate for the use environment.
- Where appropriate, provide physical locks on devices and their communication ports to minimize tampering.
- Use systematic procedures for authorized users to download version-identifiable software and firmware from the manufacturer.
- Develop and provide information to the end user concerning appropriate actions to take upon detection of a cybersecurity event.
- Provide methods for retention and recovery of device configuration by an authenticated privileged user.

5.5 Post Market Security

MANDATORY
Security risks to EBMDs are continually evolving, therefore, the manufacturers should implement a security risk management programme and documentation, for example in accordance with ISO/IEC 27001 or ISR V2, or with any other internationally accepted programme. The risk management programme should address risks related to any new or previously not discovered vulnerabilities of the EBMD, which may result in patient harm. These vulnerabilities may permit the unauthorized access, modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from an EBMD to an external recipient. It should be ensured contractually that manufacturers respond in a timely fashion to address identified vulnerabilities.

Manufacturers should have a documented methodology to identify, characterize, and assess a security vulnerability, and methods to analyse, detect, and assess threat sources. For example:

- A vulnerability might impact all of the EBMDs in a manufacturer's portfolio based on how their products are developed; or
- A vulnerability could exist vertically (i.e., within the components of a device) which can be introduced at any point in the supply chain for an EBMD manufacturing process.

These methodologies should be submitted, e.g. as part of the report card.

OPTIONAL
Manufacturers should consider the following security controls:

- Monitoring security information sources for identification and detection of vulnerabilities and risks.
- Maintaining a robust software lifecycle processes that include mechanisms for:
  - o monitoring third party software components for new vulnerabilities throughout the EBMD's entire lifecycle;
  - o design verification and validation for software updates and patches that are used to remediate vulnerabilities.
- Understanding, assessing and detecting the presence and impact of a vulnerability.
- Establishing and communicating processes for vulnerability handling.
- Using threat modelling to clearly define how to maintain safety and essential performance of a device by developing mitigations that protect, respond and recover from the security risk.
- Adopting a coordinated vulnerability disclosure policy and practice.
- Deploying mitigations that address security risk early and prior to exploitation.

Post market security information may originate from different sources, including independent security researchers, in-house testing, suppliers of software or hardware technology, health care facilities, and information sharing and analysis organizations. It is strongly recommended that manufacturers participate in a group that shares vulnerabilities and threats that impact medical devices.

5.6 Donations after end of life

MANDATORY

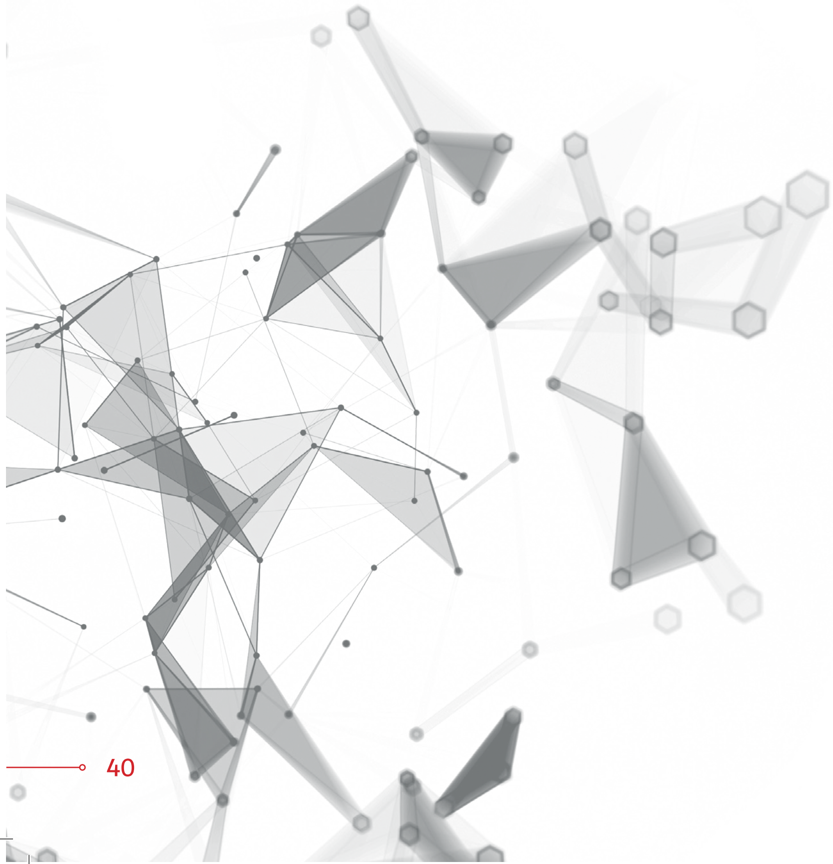
In case donations are made after the end of life of an EBMD device, the donor should ensure that the following activities take place:

- The report card belonging to the device is given over with the device;
- The report card should be used to clearly state the security controls in place, and also those that are not;
- It should be ensured that all personally identifiable information is deleted from the device. Manufactures should submit their Device Data Sanitation (DDS) procedures to DHA Bio-Medical team as part of post market security controls, or as part of contractual requirements.

DUBAI ELECTRONIC SECURITY CENTER

مركز دبي للأمن الإلكتروني

6 EXCEPTIONS



6 EXCEPTIONS

There are several cases where it might be difficult for a hospital to use this standard, such cases could be:

1. There are no devices that fulfil the criteria given in this standard, yet it is important for medical reasons to use such devices.

2. Devices or services related to the devices are provided for free by manufacturers, and they refuse to demonstrate compliance with the requirements.

In such cases, exceptions to compliance with this standard should be granted under the following circumstances:

1. Internal hospital process

The following activities should take place and should be documented:

- Identification of EBMDs in the market space that fulfil the required medical function
- Comparison of the security controls in place for these EBMDs
- The device that fulfils most of the mandatory security controls of this standard should be chosen
- Risk mitigation controls should be put in place

2. Communication with DHA

The hospital should communicate with DHA and provide the following details:

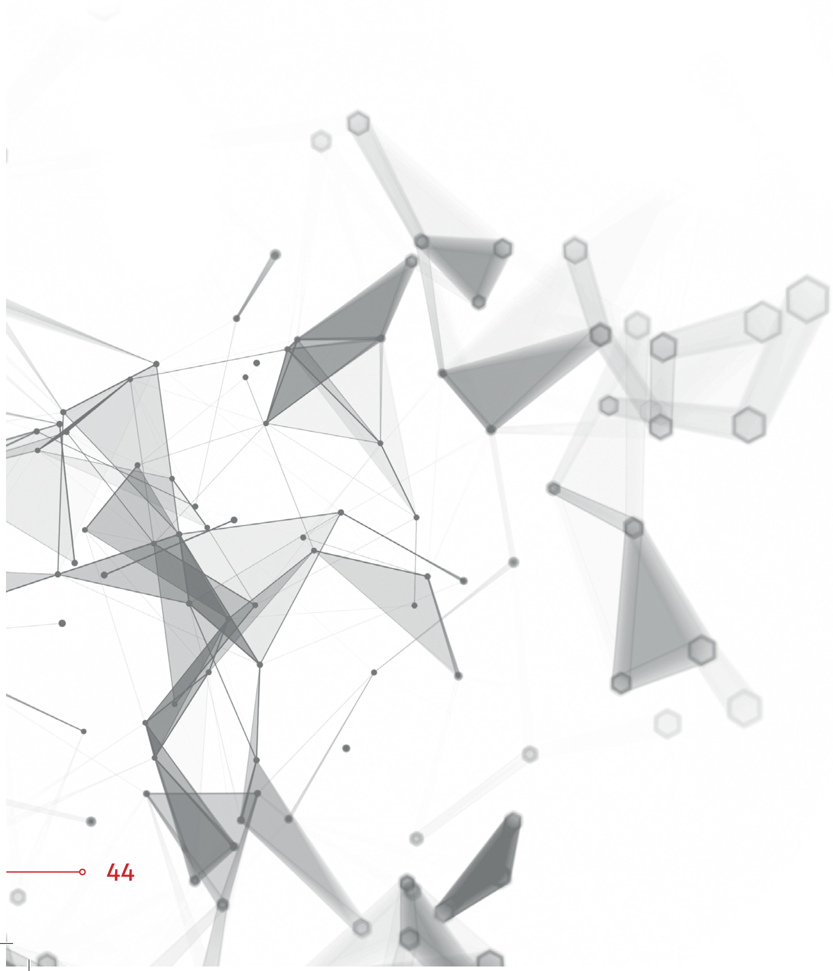
- EBMDs considered
- Results of the comparison process
- Record of the risk mitigation controls applied
- Any other relevant information
- Time frame for reply

DHA will communicate their approval/disapproval within the given timeframe.

In case of the hospital being DHA itself, DHA should keep complete records of each and every exception case. This will be verified in the ISR audit.

DUBAI ELECTRONIC SECURITY CENTER
مركز دبي للأمن الإلكتروني

7 ORGANIZATIONS AND WORKS CONSULTED IN BRIEF



7 ORGANIZATIONS AND WORKS CONSULTED IN BRIEF

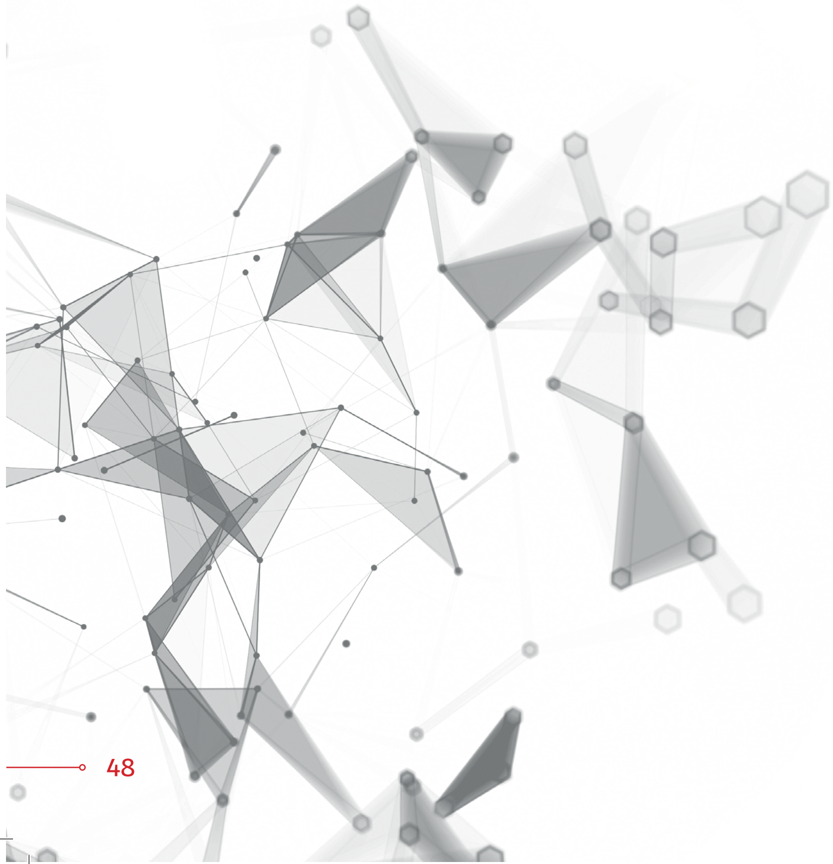
Extensive research was conducted on existing information security standards, regulations and frameworks in relation to IoT Security during the course of drafting this standard. Pertinent information security documents were identified and consulted from the following organizations among others:

- Singapore Standard Council
- IoT Security Foundation
- OWASP
- ONG-C2M2

Further various versions of several standards, regulations and frameworks related to IoT security were considered, including but not limited to:

- TR 47: 2016 IoT reference architecture for Smart Nation – Singapore Standard Council
- Connected Consumer Products Release 1.0 – Best Practice Guidelines – IoT Security Foundation
- IoT Security Guidance - OWASP
- Strategic principles for the security of IoT - OWASP
- Cybersecurity Capability Maturity Model (ONG-C2M2) – Oil and Natural Gas

ANNEXES



ANNEX A EBMD SECURITY CONTROLS BASED ON THE IOT SECURITY STANDARD

A.1 Overview

This annex to the EBMD Security Standard provides mandatory and recommended controls for the security of Biomedical Devices (EBMD) in the city of Dubai, the controls are applicable based on the class of the EBMD as described in section 4. This annex is based on the IoT Security Standard developed by DESC; it has been adapted to fit its application to EBMDs.

A.2 Underlying Models

A.2.1 EBMD SECURITY MODEL

The basis of the security model applied in this standard is derived from the international standard ISO/IEC 27001 and the local Information Security Regulation (ISR). These standards provide an organizational security framework in which a EBMD device can operate securely

In addition, a layer-based approach is used to describe the key aspects of information security for a EBMD device. The layers considered are:

- Network Layer - this layer addresses all information security controls that can be implemented through the network, such as network access control, logging and monitoring, and segregation.
- Device Layer – this layer addresses information security controls that can be implemented on the EBMD device itself. As EBMD devices are very diverse such controls can range from simple features, such as password protection through to more complex features, such as encryption.

Both the organizational security framework, and the controls applied on the device and application layers are critical for proper securing of EBMD. For example, if, for any reason, breaches occur in the device or network layer, the incident management process provided by the organizational security framework can ensure proper management of these incidents.

A.2.2 RISK ASESSMENT

Not all EBMD devices have the same requirements for security, how much a device needs to be secured is a direct result of how and where the EBMD device is used. Most EBMD devices will require the application and configuration of advanced security features (see also classification – section 5). Therefore, the advanced security controls that are applied to a EBMD device should be determined through an assessment of the risks involved.

A.2.3 HOSPITALS

The use of ISR and/or ISO/IEC 27001 provides the security framework for the EBMD devices. Ensuring that a EBMD device operates in a secure environment minimizes the security issues that might arise from improper implementation or operation of security controls on the device or network layer.

Hospitals should be encouraged to implement ISR and/or ISO/IEC 27001 and should carry out a risk assessment to determine appropriate security controls for their EBMD devices.

A.3 Generic Mandatory EBMD Security Controls

This section describes generic mandatory security arrangements that organizations shall follow when developing secure EBMD products. The controls listed below form the basic set that each organization using EBMD devices shall implement. The detailed implementation should take into account the results of the risk assessment mentioned in Section 2.2 above.

No.	The mandatory controls for EBMD devices are listed below:
1	Ensure that the defined security measures are implemented/active, even when a EBMD device is facing some technical/operational disruption.
2	Ensure that proven security solutions recognized by the security community are applied to the EBMD device.
3	Ensure that all security-relevant activities (e.g. access to and/or modification of the device or information on it) can be logged and monitored.
4	Ensure that security events and incidents can be detected and recorded for necessary corrective action.
5	Provide regularly updated disclosure of vulnerabilities
6	Ensure that a secure booting process is in place for the EBMD device.
7	Ensure, (for example by code signing*) that malicious code cannot be injected into the EBMD device.
8	Disclose information regarding the replacement, removal or addition of any component in the supply chain of an EBMD device that is currently approved and provided in the market.
9	The security guidelines and risk assessments should be readdressed whenever any update is introduced to the existing EBMD devices.
10	Ensure that compromised or infected devices are identified and revoked in order to avoid having other functionalities of the system affected.
11	Inform users/buyers of EBMD devices about the expected life period of a given EBMD device as well as the risks/ issues associated with using it beyond its usability date.

** Code signing is the method of using a certificate-based digital signature to sign executables and scripts in order to verify the author's identity and ensure that the code has not been changed or corrupted since it was signed by the author.*

12 Clearly indicate on the EBMD device itself, and/or its packaging, its dependencies on any other systems/devices.

13 Provide a secure and reliable method to transfer the ownership of a EBMD device from one person to another.

14 Ensure that the information on the device can completely be wiped or destroyed whenever it is needed, as part of information protection, and a method of secure destruction.

15 Ensure that any sensitive personally identifiable information can be anonymized or removed where necessary.

16 Access to EBMD devices should be strictly controlled, unauthorized access should be detected.

17 A secure authentication method should be implemented on the EBMD device.

18 Ensure that only up to date software is used in conjunction with EBMD devices; updates of the software should be possible, when necessary. Allow only authorized sources to provide such updates.

19 Ensure that the existing connectivity can be maintained under all circumstances, and that it is not possible to introduce other communication paths.

20 Ensure that health-specific security and privacy standards are adhered to.

21 Ensure that all communication and data storage related to EBMD devices are encrypted, where necessary, and that the encryption algorithm used is adequately strong.

22 Put appropriate network segregation in place (based on risk assessment results).

23 Ensure that all connections are removed from any EBMD device that has been removed from the network.

A.4 Optional Advanced EBMD Security Controls

The following advanced EBMD security controls for EBMD devices should be considered and applied on the basis of the results of the risk assessment.

A.4.1 SECURE WEB INTERFACE

- Ensure that the BDM web interface has been tested for XSS, SQLi and CSRF vulnerabilities and OWASP Top 10 Security Vulnerabilities
- Ensure that the EBMD interface uses Secure Coding (for example prevention on the use of old Java code, vulnerable J-Query plugins etc.).

A.4.2 AUTHENTICATION/ AUTHORIZATION

- Ensure that the EBMD uses strong password authentication, including:

  o Brute-force attack mitigation

  o Disabling the use of default or hardcoded passwords

  o Enforcing password best-practices

  o Disallowing display of user credentials on login interfaces

  o Enforcing thresholds and incremental delays for invalid password attempts

- Ensure that, where applicable, user roles are properly segregated.
- Ensure that the EBMD supports two-factor authentication using OTP (SMS) or backend integrated with Radius Server.
- Ensure that the EBMD supports secure password recovery mechanisms only during boot level.
- Ensure that the EBMD device on boarding process has met the requirements of secure authentication and authorization.

A.4.3 COMMUNICATION SECURITY

- Ensure that all EBMD devices operate with a minimal number of network TCP/UDP ports active. Ensure that the EBMD devices is pre-hardened and unused ports are disabled.
- Ensure that the EBMD device supports a trust anchor, a secure hardware technology that stores and processes cryptographic secrets such as Pre Shared Keys (PSK) or asymmetric keys (PKI). Trust anchors can be used to authenticate peers during network communications.
- Ensure that a EBMD device provides Separation of Duties such as keys to identify varying components or services. For example, one set of cryp-

tographic keys could represent a firmware update service, while a second set of cryptographic keys could represent a "push" service.

- Ensure that the EBMD device supports the requirement to ensure the EBMD device can operate in isolation with the same level of security in case the connectivity.
- Ensure that the encryption used for the communication to and from the EBMD device is adequately secure.
- Ensure that the EBMD device supports EBMD Device Personalization such as cryptographically unique identities.
- Ensure Remote Access Administration of EBMD Devices is not available over the public interfaces or applications (API). Use of a separate communication channel for Remote Administration is highly recommended.
- Apply industry standard and accepted encryption practices and avoid proprietary protocols, in line with the risk assessment results.

A.4.4 HARDWARE SECURITY

- Employ a hardware-based immutable root of trust.
- Use hardware that incorporates security features to strengthen the protection and integrity of the device – for example, specialized security chips / coprocessors that integrate security at the transistor level, embedded in the processor, providing, among other things, a trusted storage of device identity and authentication means, protection of keys at rest and in use, and preventing unprivileged from accessing to security sensitive code. Protection against local and physical attacks can be covered via functional security.

A.4.6 DEVICE MANAGEMENT

Ensure that the EBMD device provides mechanisms to detect malicious and anomalous activity or integrate easily into device side malware protection or anomaly detection products.

- Ensure that EBMD devices are able to detect and resist attacks from the edge including spoofing, replay, and excessive communications.
- Ensure that remote "Firmware over the Air", Remote "Administration", Remote "Patching" and other such EBMD device services are secured and not accessible publically or over the Internet.

- Ensure that the EBMD device supports disabling debugging and test technology interfaces.
- Apply a secure mechanism to decommission EBMD devices and revoke communication securely.

A.4.7 SOFTWARE/ FIRMWARE

- Ensure that update files are encrypted and that the files are also transmitted using encryption
- Ensure that update files are signed and then validated by the device before installing
- Ensure that the EBMD device has the ability to implement scheduled updates
- Ensure that the EBMD device supports EBMD Device Image/Firmware Validation using secure cryptographic mechanisms to ensure the EBMD device firmware has not been tampered with. This can be integrated as part of the trust anchor.
- Ensure that automatic firmware updates do not modify user-configured preferences, security, and/or privacy settings without user notification.

A.4.7 SECURE STORAGE

- Sensitive data on the EBMD device edge is liable to theft or exposure unless it is stored with proper security considerations. Ensure that some form of secured local storage for data is offered, that protects it from local malicious applications, compromised operating systems, or malicious owner/operator. Sensitive data can include sensor reading, configuration settings, authentication credentials, or cryptographic keys.

ANNEX B DEFINITIONS

ACCESS CONTROL

Mechanism to enable authorized people to access physical or digital entity resources, while preventing unauthorized people from doing the same.

ASSETS

Economic resources that are tangible or intangible, capable of being owned or controlled to produce value, and held to have positive economic value.

AUTHENTICATION

Act of verifying a claim of identity.

Note It is usually one or more of the following: something you know (password), something you have (identification card) or something you are (finger print).

AUTHORIZATION

Mechanism that verifies that the authenticated subject can carry out the intended action.

AVAILABILITY

Property of being accessible and usable upon demand by an authorized entity

ELECTRONIC BIOMEDICAL DEVICES (EBMD)

Any electronic device, appliance, or software —whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application—intended by the manufacturer to be used for human beings for the purpose of:

o Diagnosis, prevention, monitoring, treatment, or alleviation of disease;

o Diagnosis, monitoring, treatment, alleviation, or compensation for an injury or handicap; or

o Investigation, replacement, or modification of the anatomy or of a physiological process.

CHANGE MANAGEMENT

Formal process for directing and controlling alterations to the information processing environment.

Note Its objectives are to reduce the risks posed by changes to the information processing, environment and improve the stability and reliability of the processing environment as changes are made. The change management process ensures that a change is: Requested, Approved, Planned, Tested, Scheduled, Communicated, Implemented, Documented and Reviewed after the change.

COMPLIANCE

Act of adhering to, and demonstrating adherence to, a standard or regulation (international, national or internal).

CONFIDENTIALITY

Property that information is not made available or disclosed to unauthorized entities.

CONFIGURATION MANAGEMENT

IT service management process that tracks all the individual configuration items (IT Assets) in an IT system.

Note This IT system might be as simple as a single server or an entire IT department.

CRITICAL INFORMATION INFRASTRUCTURE (CII)

Assets, including organizations, which provide essential services that underpin UAE’s society.

Note The Nation possesses numerous key resources, whose exploitation or destruction by any attacks could cause catastrophic effects, or could profoundly affect our national prestige and morale. In addition, there is critical infrastructure so vital that its incapacitation, exploitation, or destruction through attacks could have a debilitating effect on security and economic well-being.

CRYPTOGRAPHY

Discipline that embodies principles, means, and mechanisms for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use.

EVENT

Any observable occurrence in a system or network.

Note Depending on their potential impact, some events need to be escalated for response.

IDENTITY

Set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager’s responsibility, is sufficient to distinguish the entity from any other entities.

IDENTITY AND ACCESS MANAGEMENT (IAM)

The creation and management of identities for entities that may be granted logical or physical access to the organization’s assets.

Note Access to the organization’s assets, commensurate with the risk to critical infrastructure and organizational objectives, needs to be controlled.

INCIDENT

Violation or imminent threat of violation of cyber security policies, acceptable use policies, or standard security practices.

INFORMATION

Any information, which can exist in many forms, such as printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation.

INTEGRITY

Property of accuracy and completeness.

IOT DEVICE

Any device that connects to a network and has the ability to receive and/or transmit data.

Note IoT devices might fall into three categories: sensors, actuators or gateways. Examples of IoT devices are: thermostats, door locks, fridges, and sensors in cars.

IOT PLATFORM

Whole set of components of IoT devices, gateways, and infrastructure that supports the operation of the IoT devices.

LOGGING

Automated recordkeeping (by elements of an IT or OT) of system, network, or user activity.

Note Logging may also refer to keeping a manual record (for example a sign-in sheet) of physical access by personnel to a protected asset or restricted area, although automated logging of physical access activity is commonplace.

MALICIOUS CODE

A code to infiltrate a computer system without the owner’s informed consent to make it unavailable, steal information or use it to attack other computers.

Note This includes computer viruses, worms, Trojan horses, spyware, dishonest adware, crime ware, rootkits, and other malicious or unwanted software.

MONITORING

Collecting, recording, and distributing information about the behavior and activities of systems and persons to support the continuous process of identifying and analyzing risks to organizational assets and critical infrastructure that could adversely affect the operation and delivery of services.

MULTIFACTOR AUTHENTICATION
Concept of using two or more factors to achieve authentication.

Note Factors include (i) something you know (e.g. password/PIN), (ii) something you have (e.g. cryptographic identification device, token), (iii) something you are (e.g. biometric), or (iv) somewhere you are (e.g. GPS token).

NETWORK ARCHITECTURE
Framework that describes the structure and behavior of communications among IT and/or OT assets and prescribes rules for interaction and interconnection.

PHYSICAL ACCESS CONTROL
Controls that monitor and control the environment of the work place and computing facilities.

Note They also monitor and control access to and from such facilities. For example: doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks, etc. Separating the network and work place into functional areas are also physical controls.

RISK
Quantifiable likelihood of potential harm that may arise from a future event.

RISK ASSESSMENT
Step in the risk management process to determine the qualitative or quantitative value of risk in relation to a recognized threat.

Note Quantitative risk assessment requires calculations of two components of risk; R, the magnitude of the potential loss L, and the probability p; that the loss will occur.

TRUSTED COMPUTING BASE (TCB)
A suite composed of hardware, software, and protocols that ensures the integrity of the endpoint.

VULNERABILITY ASSESSMENT
Systematic examination of an IT or product to determine the adequacy of cyber security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed cyber security measures, and confirm the adequacy of such measures after implementation.

ANNEX C INTERNATIONAL CLASSIFICATION MODELS

A number of countries have established a classification for biomedical devices; all concepts applied are using the same basis: the potential negative impact a problematic EBMD might have on the patient, and are relatively similar. The details of the different classification schemes are relatively complex, please refer to the documents cited below to get a more in-depth overview.

- Australian Regulatory Guidelines for Medical Devices, Section 4. Classification of medical devices, Version 1.1. 2011
- European Union MEDICAL DEVICES Guidance Document – Classification of medical devices, June 2010
- Medicines (Database of Medical Devices) Regulations 2003 , New Zealand
- Title 21 of the Code of Federal Regulations (CFR), Parts 862-892 – Classification in US, approved by FDA
- Schedule 1, Part 1 of the Canadian Medical Devices Regulations (CMDR) SOR/98-282

The following overview depicts the situation:

Table 1 Classification of biomedical devices in Canada and the EU

Canada	Description	EU	Compliance
Class IV	In depth scrutiny	Class III	Certificate of conformity
Class III	In depth scrutiny	Class II b	Certificate of conformity
Class II	Manufacturer's declaration	Class II a	Certificate of conformity
Class I	No license needed	Class I	Self-certification*

Table 2 Classification of biomedical devices in the US and Australia

US	Description	Australia	Associated Risk
Class II	Class II + pre-market approval	Active implantable medical devices (AIMD)	High
Class II	Class I + special controls	Class III	High
Class I	General controls	Class II b	Medium - High
		Class II a or Class I	Low - Medium
		Class 1*	Low

The classification labels and details that have been chosen for this standard makes use of the concepts described in

- Australian Regulatory Guidelines for Medical Devices, Section 4. Classification of medical devices, Version 1.1. 2011
- European Union MEDICAL DEVICES Guidance Document – Classification of medical devices, June 2010