WHISTLEBLOWING POLICY

(hereinafter referred to as the "**Policy**")

Preamble

The present whistleblowing policy is established in accordance with the law of 16 May 2023 transposing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (hereinafter referred to as the "**Law**").

The Policy applies within the company B Medical Systems S.à r.l., with registered office at 17, op der Hei, L-9809 Hosingen, registered with the Luxembourg Trade and Companies Register under the number B91535 (hereinafter referred to as the "**Employer**" or the "**Company**").

Its purpose is to provide information and to indicate the procedures for collecting, processing and following up internal reports made in good faith by the reporting person.

The present Policy is applicable as of 1 September 2023. The Employer reserves the right to modify and amend the content of this Policy at any time.

The Policy is uploaded on the Company's Common Folder and is to be found under the following path COMMON > HR-Common > B Medical Information > Compliance > Compliance Policies > Whistleblowing Policy. The Policy is also displayed on a bulletin board at the Company's premises. A training session to explain the details of this Policy is held every month for new joiners. A copy of this Policy is furthermore available on the platform of the compliance software tool "NAVEX", that employees can access to report a breach (please see below for further details).

Article 1: Definitions

Term	Definition
Breach(es)	Acts or omissions that are unlawful or contrary to the object or purpose of national law or directly applicable provisions of EU law.
External report	The oral or written communication of information about breaches to the competent authority.
Facilitator	A natural person who assists a reporting person in the reporting process in a work-related context, and whose assistance should be confidential.

Information on Breaches	Information, including reasonable suspicions, about actual or potential breaches, which occurred or are very likely to occur in the organisation in which the reporting person works or has worked or in another organisation with which the reporting person is or was in contact through his or her work, and about attempts to conceal such breaches.
Internal report	The oral or written communication of information about breaches within the Company.
Person concerned	Natural or legal person who is referred to in the report or public disclosure as the person to whom the breach is attributed or with whom that person is associated.
Public disclosure or disclose publicly	The making of information about breaches available in the public domain.
Report or reporting	The oral or written communication of information about breaches.
Reporting person	Any natural person who reports or publicly discloses information on breaches acquired in the context of his or her work-related activities.
Retaliations	Any direct or indirect act or omission, which occurs in a work-related context, is prompted by internal or external reporting or by public disclosure, and which causes or may cause unjustified detriment to the reporting person.
Reporting Tool	Compliance software made available by the Company to report Breaches
Work-related context	Current or past work activities in the public or private sector through which, irrespective of the nature of those activities, persons acquire information on breaches and within which those persons could suffer retaliation if they reported such information.

Article 2: General provisions - Principles

Who can be a Reporting person? Present or former employees (including part-time and fixed-time workers), but also candidates, trainees (paid or unpaid), volunteers, self-employed persons, shareholders, directors or managers, as well as any person working for contractors, subcontractors and suppliers.

The Reporting person must report Breaches in good faith, meaning he must have "*reasonable grounds to believe that the information on breaches reported was true at the time of reporting*" (article 4 of the Law). All national law is covered.

The Reporting Tool should be used by the employees (including part-time and fixed-time workers), students, trainees, apprentices and temporary workers of the Company when reporting a Breach, by following the instructions as displayed on the NAVEX platform made available by the external service provider (link provided under section 4.1. below).

External parties, such as suppliers, customers, distributors, agents etc., can report a Breach via the generic e-mail address, as displayed on the Company's website (https://www.bmedicalsystems.com/en/).

The information reported must have been collected lawfully, in compliance with existing legal provisions.

Information on Breaches must be reported and will be processed in accordance with article 4 of this Policy.

Persons wishing to report Breaches are encouraged to give priority to internal reporting (in particular by using the Reporting Tool) within the Company before any external reporting to a competent authority.

Please note that the Company has a separate policy on moral and sexual harassment. Anyone who believes that he / she has been the victim of, or has witnessed, acts of moral or sexual harassment within the Company is encouraged to report an incident under this separate policy applicable within the Company and specifically dedicated to moral and sexual harassment.

The policy on moral and sexual harassment in the workplace is uploaded on the Company's Common Folder and is to be found under the following path COMMON > HR-Common > B Medical Information > Compliance > Compliance Policies > Moral and Sexual Harassment Policy. The Policy is also displayed on a bulletin board at Company's premises.

Article 3: Duty of guarantee and confidentiality

3.1. The internal reporting channels provided for in article 4 of the Policy are designed, established and managed in a secure manner that guarantees the strict confidentiality of the identity of the Reporting person, of any third party mentioned in the report and of all information and data contained in the Report.

The entire procedure described in article 4 of this Policy will be conducted confidentially, objectively and impartially.

The persons involved in this procedure scrupulously undertake to respect the confidentiality of the information and data brought to their attention. Failure to do so may result in disciplinary action.

3.2. The identity of the author of the Report, including any information from which the identity of the latter may be directly or indirectly deduced, may not be disclosed without the express consent of the latter to persons other than the authorised and competent members of staff provided for in article 4 of the Policy.

By way of derogation from the preceding paragraph, the identity of the author of the Report and any other information referred to in the preceding paragraph may be disclosed only where this is a necessary and proportionate obligation imposed by the amended law of 8 June 2004 on freedom of expression in the media or by European Union law in the context of investigations carried out by national authorities or in the

context of legal proceedings, in particular with a view to safeguarding the rights of defence of the person concerned.

Article 4: Procedure to follow in case of internal report

The internal reporting procedure described hereafter applies to all of the Company's employees (including part-time and fixed-time workers), as well as students, trainees, apprentices and temporary workers.

External parties who have a professional link towards the Company (in particular suppliers, distributors, customers, contractors etc.) are requested to report a Breach via the generic e-mail address displayed on the Company's website.

4.1. Rules for the internal report of breaches

1. *Reporting channel*:

The Breach must be reported in English or in French in sufficiently precise terms to be admissible.

The Reporting person must report in good faith in the following manner:

- in writing via the platform NAVEX (link: https://secure.ethicspoint.eu/domain/media/en/gui/107004/index.html); or

- via the secure telephone hotline as displayed on the NAVEX website. Complete and accurate minutes of the conversation will be drawn up by the person handling the phone call, and made available to the Director, Human Resources, the Director, Legal & Compliance and the Senior Vice President, General Counsel & Secretary for further processing. The telephone conversation will not be recorded; or

- in person by requesting a physical or e-meeting with the Director, Human Resources, the Director, Legal & Compliance and the Senior Vice President, General Counsel & Secretary. Complete and accurate minutes of the conversation will be drawn up by the Director, Legal & Compliance.

2. *Content of the Report*:

The report (including via the Reporting Tool) shall include at least the following information:

- the identity, the function and the contact details of the Reporting person;
- the subject of the Report;
- the identity of the person(s) to whom the report relates;
- a precise and detailed description of the facts (dates, witnesses, etc.);
- any information or any document, in whatever form or on whatever support, that may support the Report.

3. *Anonymous Report* :

The Reporting person may issue an anonymous Report, although identified reports are strongly encouraged. Please note that all reports, even if anonymous, must be made in good faith.

An anonymous Report will only be accepted in exceptional circumstances. In order to be taken into account, the written Report must be sufficiently precise and include at least the information set out in point 2 above (except the identity, the function and the contact details of the Reporting person), as well as an explanation

of the exceptional circumstances justifying an anonymous report. It is at the sole discretion of the Company to accept the exceptional circumstances justifying the anonymous reporting and to deal with the Report.

If the Director, Human Resources, the Director, Legal & Compliance and the Senior Vice President, General Counsel & Secretary receiving the written report considers it sufficiently precise and the exceptional circumstances justified, the anonymous Reporting person must be willing to answer any questions deemed useful in the context of processing the Report.

Failing this, the Company will not be obliged to deal with the anonymous Report.

If all requirements for an anonymous Report are met and any additional questions are answered, the Report will be processed and followed up in the same way as non-anonymous Reports.

4. *Acknowledgement of receipt of the Report:*

An acknowledgement of receipt of the Report will be sent to the Reporting person as soon as possible and at the latest within 7 days of receipt of the Report.

5. *Admissibility of the Report*:

To enable the Company to process and follow up the Report, it must be phrased in sufficiently precise terms. Failing this, the Report will not enable the Employer to fulfil its obligations and the Company may decide either to file the Report with no further action or to request additional information.

Where the report is sufficiently precise, it will be dealt with in accordance with the following point.

4.2. Processing and follow-up of the Report

1. *Contemplated follow-up measure(s):*

The Director, Human Resources, the Director, Legal & Compliance and the Senior Vice President, General Counsel & Secretary will decide on the measures to be taken in the light of the information reported by the Reporting person. The Reports may be discussed, for information purposes only, during the meetings of the Compliance Committee in strict confidentiality as long as no personal data are revealed. The Compliance Committee is composed of the VP, CEO – B Medical Systems, the VP, Deputy CEO – B Medical Systems, the Senior Director – CFO B Medical Systems, Azenta Representatives and the Director Legal & Compliance. The composition may be subject to change in case of conflict of interest or if one or more members are directly or indirectly involved in the Breach. In case the Report concerns actions of the Director, Human Resources, then the Report will be forwarded to the Director, Legal & Compliance and to the Senior Vice President, General Counsel & Secretary. In case the Report concerns actions of the Director, Legal & Compliance, then the Report will be forwarded to the Director, Human Resources and to the Senior Vice President, General Counsel & Secretary. In case the Report concerns actions of the Senior Vice President, General Counsel & Secretary, then the Report will be forwarded to the Director, Human Resources and to the Director, Legal & Compliance.

The contemplated measures may include in particular:

- the referral of the Reporting person to the appropriate person or department within the Company in the event of inadmissibility;

- the closure of the procedure, when the elements reported do not make it possible to conclude that a Breach has occurred, in the event of a manifestly minor Breach requiring no further action other than the closure of the procedure, due to insufficient evidence or for other reasons that will be

specified to the Reporting person (the procedure will be closed, for example, in the event of repeated reports that contain no significant new information in relation to any previous report);

- the opening of an investigation when the reported elements require so (please refer to article 4.2. point 2 of the Policy);

- sanctions against the perpetrator(s) of the Breach when the reported elements are sufficient in themselves to come to the conclusion that a Breach has occurred (please refer to article 6 of the Policy);

- the referral to a competent authority for further investigation, insofar as this information would not prejudice the internal investigation or the investigation or infringe the rights of the person concerned.

Information on the contemplated or taken measures as part of the follow-up and on the reasons for this follow-up must be provided within a reasonable timeframe, and at the latest within 3 months of the acknowledgement of receipt of the Report or, in the absence of an acknowledgement of receipt, within 3 months of the expiry of a period of 7 days following the receipt of the Report.

The Reporting person will be kept informed on a regular basis, and at their reasonable request, of the progress of the processing of the report. The Reporting person may also be asked to provide any additional information deemed necessary to process the Report.

2. *Investigation*

a) If the reported elements require so, an investigation will be carried out by the Director, Human Resources, the Director, Legal & Compliance and the Senior Vice President, General Counsel & Secretary as soon as possible, depending on the availability of all parties and the complexity of the case.

The Director, Legal & Compliance, the Director, Human Resources and the Senior Vice President, General Counsel & Secretary reserve the right to be assisted by an external service provider if necessary.

As part of the investigation, individual interviews may be conducted with the following people:

- the Reporting person;
- the alleged perpetrator(s) of the Breach;
- if necessary , any person mentioned in the Report or any person who can provide clarification on the reported facts (work colleagues, superior, etc.).

A report of each interview will be signed and dated by the person interviewed and the persons who conducted the interview.

These exchanges are intended to supplement any documents and information gathered to enable a decision to be taken on the reported Breach.

b) On the basis of the reports and other elements gathered, the Director, Legal & Compliance, the Director, Human Resources and the Senior Vice President, General Counsel & Secretary will draw up the final investigation report in order to determine whether or not the reported Breach has been established and they will decide on the measures to be taken.

The conclusions of the investigation, i.e. whether or not a Breach has been established, will be communicated to the Reporting person and to the perpetrator(s).

The reports of the interviews and any documents and information gathered remain strictly confidential. They may, if necessary, be forwarded to the competent authority at its request or to the courts in the event of a dispute.

c) If the Breach is established, appropriate sanctions will be taken against the perpetrator(s) in accordance with article 6 of the Policy.

If the Breach is not established, the procedure is closed.

Article 5: External report to a competent authority

The Reporting person may lodge an external Report to the competent authority and in accordance with the reporting channels and procedures set up by the competent authority:

- either after having made an internal Report in accordance with this Policy;
- or directly if it is impossible to effectively remedy the Breach internally or if there is a risk of retaliation against the Reporting person.

Under the Law, the Reporting person is encouraged to privilege internal reporting channels before reporting externally.

Article 6: Sanctions against the perpetrator(s) of the Breach

When a Breach is established, appropriate sanctions will be taken against the perpetrator(s) of the Breach:

- If the perpetrator of the Breach is an employee of the Company, he/she will be subject to a disciplinary sanction which may go as far as dismissal with immediate effect;

- If the perpetrator of the Breach is the holder of a corporate mandate (director, manager, daily manager etc.) of the Company, he or she may be revoked, with immediate effect as the case may be;

- If the perpetrator of the Breach is a customer or a supplier, the Company will inform the co-contracting company and discuss with it the measures to be taken (which may range from replacing the customer's/supplier's staff to terminating the contractual relationship).

The perpetrator of the Breach is informed that, depending on the nature and the extent of the Breach, legal, criminal and/or administrative proceedings may be taken against him/her.

Article 7: Protection of the Reporting person

1. The Reporting person who makes a Report in good faith in accordance with this Policy and the legal provisions in force shall not be subject to retaliations for the reported facts.

2. However, any Report which is not made in good faith, which contains misleading information or which is made in particular with the intention of harming the Company or of harming a specific person may be subject to disciplinary sanctions up to a dismissal with immediate effect.

In addition, pursuant to article 27(5) of the Law, a Reporting person who has knowingly reported or publicly disclosed false information may be subject to a sentence of imprisonment of 8 days up to 3 months and a fine of between EUR 1,500 and EUR 50,000.

The author of a false Report may also be held civilly liable (including in the case of a Report made when its author was aware of the falseness of the information reported) and the Employer may claim damages for the loss suffered before a competent court.

Finally, it should be remembered that the person targeted by false accusations benefits from a personal action for defamation or slanderous denunciation against the reporting employee.

3. The protection measures provided for in point 1 also apply to facilitators and third parties who are related to the Reporting person and who are at risk of retaliations in a work-related context (e.g. colleagues, relatives of the Reporting person).

Article 8: Processing of personal data

1. Any processing of personal data under this Policy and the Law shall be carried out in accordance with:

- the Regulation (EU) 2016/679 of 27 April 2016 (General Data Protection Regulation, hereinafter referred to as "**GDPR**");
- the law of 1 August 2018 on the protection of individuals with regard to the processing of personal data in criminal matters as well as in matters of national security;
- the GDPR Policies implemented within the Company.

2. Personal data that is clearly not relevant to the processing of a specific Report shall not be collected or, if collected accidentally, shall be deleted immediately.

3. In accordance with the law of 16 May 2023 and the GDPR, the storage period for documents in connection with a Report of a Breach will be determined on a case-by-case basis depending on the nature of the reported Breach or misconduct.

ACKNOWLEGMENT OF RECEIPT

This Policy forms an integral part of the Employee's employment contract.

I, the undersigned, acknowledge that I have read the Company's Whistleblowing Policy and undertake to comply with its contents.

Signed in Hosingen, on [date]

Signature of the Employee