Bioventus, LLC
4721 Emperor Blvd.
Durham, NC 27703 USA

1-919-474-6700
1-800-396-4325

IT Policy and Procedure

AI Tool Acceptable Use Policy	SmartSolve #	POL-000091 [A]
	Page:	Page **1** of **4**

Purpose

This policy establishes specific requirements for the use of AI Tools at Bioventus. The information technology resources at Bioventus support the business activities of the company and the use of these resources is a privilege. As a user of AI Tools you are required to behave in a responsible, ethical, and legal manner.

Bioventus recognizes that, in addition to their many benefits, AI tools may pose risks to our operations and the individuals with whom we engage. We are committed to protecting the confidentiality, integrity, and availability of all company, customer, and [partner/user/employee/patient] data, and to the informed and responsible use of AI tools in compliance with applicable laws. In addition, this policy adheres to and supports the Bioventus *Global Privacy Program.*

Scope

The AI Tool Acceptable Use Policy applies to:

- all employees, contractors, third-parties and guests who working on behalf of Bioventus with access to Bioventus' personal, proprietary, confidential, or trade secret information, information systems, or any material non-public information.
- all information that is owned by or entrusted to Bioventus.

Responsibilities

All Bioventus employees, contractors, third parties or guests are expected to:

- Understand and comply with the AI Acceptable Use policy;
- Be responsible for the information resources provided to you by Bioventus;
- Exercise good judgement in the use of Bioventus' technological and information resources;
- Acknowledge AI Policy.

Manager: In addition to the above, each manager has a responsibility to:

- Ensure his/her employees understand and adhere to the AI Acceptable Use Policy
- Review and if appropriate, address adherence issues of his/her employees through additional training
- Report violations of this policy to IT security

AI Tool Acceptable Use Policy	SmartSolve #	POL-000091 [A]
	Page:	Page **2** of **4**

Definitions

Bioventus Information: information that Bioventus collects, possesses, or has access to, regardless of its source including information contained in hard copy documents or other media, communicated over voice or data networks, or exchanged in conversation.

Protected Health Information (PHI): health information, including demographic information, created or received by Bioventus that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual and that identifies or can be used to identify the individual.

Personally Identifiable Information (PII): Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

Artificial Intelligence (AI): the theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages.

Unauthorized Access: looking up, reviewing, copying, modifying, deleting, analyzing, or handling information without proper authorization or legitimate business need.

Policy

All Bioventus employees, contractors, third parties or guests are expected to adhere to the following standards:

1) **Evaluation of AI tools:** Prior to using an AI tool for business purposes, contact [Legal/IT/IT Security/Compliance] to confirm adequate security, privacy, and related protections. Do not download or otherwise integrate an AI tool into the Bioventus' information systems without prior approval from [IT/IT Security/Compliance] for such integration. For clarity, approval to use an AI tool does not grant approval to integrate that tool into the Company environment, which requires a separate approval. Approved AI tools must be used as directed in this Policy.

2) **Data Protection:** Do not upload or input any data into an AI tool that is confidential, proprietary, or protected by applicable laws. This includes data related to [customers, employees, partners, patients, users, etc.]. The following types of data should never be uploaded, shared, or used in querying or otherwise using a third-party AI:

    a. **Personal Data, Personal Information (PII), or Protected Health Information (PHI)** (*see also* [The Bioventus Global Privacy Program]).
    b. **Material Non-Public Information** (see [Insider Trading Compliance Policy])
        i. Corporate earnings and earnings forecasts
    c. **Confidential or Trade Secret Information** (*see also* [Information Classification Policy])
    d. **Intellectual Property and/or Proprietary Source Code (***see also* [Information Classification Policy])

Bioventus, LLC
4721 Emperor Blvd.
Durham, NC 27703 USA

1-919-474-6700
1-800-396-4325

3) **Configure the Tool for Maximum Confidentiality:** Reputable AI tools provide data control settings to limit how the AI uses information input by users. Data controls should be configured to prevent the AI from utilizing user inputs to train the AI, to the extent allowed by the AI provider. History should also be set to delete frequently and automatically. Always employ strong passwords but do not use the same passwords to authenticate to the AI as you use to sign in at work.

4) **Before Entering Information Consider Downstream Consequences:** Before entering information into an AI, ask yourself whether Bioventus or individuals would be harmed if the information appeared publicly. If so, do not enter the information into an AI tool without prior approval from [Legal/IT/IT Security/Compliance].

5) **Use Caution in Trusting Results:** Because AI is still a developing technology, there are concerns about the accuracy of results, built-in biases against marginalized groups, and a lack of transparency relating to the sources from which the AI generates its content. Additionally, for AI that generates images, audio, or video, using such generated content could give rise to legal risks related to IP infringement. Do not rely exclusively on third-party AI tools in decision-making. Always validate results against vetted, trusted sources. Do not publish generated content on Bioventus channels without prior approval from [Legal/Marketing/Compliance].

6) **Using Company Purchased or Developed AI:** Always contact [Legal/IT/IT Security/Compliance] before launching an AI application on behalf of Bioventus. For example, before deploying an AI-powered chatbot to improve website engagement, work closely with [Legal/IT/IT Security/Compliance] to ensure it complies with applicable laws and meets Bioventus security standards. Users interacting with an AI must be informed that they are interacting with an AI system and that interactions may be recorded.

Bioventus, LLC
4721 Emperor Blvd.
Durham, NC 27703 USA

1-919-474-6700
1-800-396-4325

IT Policy and Procedure

Enforcement

Any person who violates this Policy may be subject to appropriate disciplinary action or other remedial measures up to and including termination of employment if warranted under the circumstances and permissible under applicable law.

It is our expectation that all Bioventus employees and those working on our behalf will comply with the requirements of this Policy, our compliance policies and standard operating procedures. You are required to report any actual or suspected violation of Bioventus' policies related to this Policy to your manager or a Human Resources or Compliance partner.

Bioventus does not tolerate retaliation, including by threats, intimidation or harassment, against anyone who in good faith reports any concerns or possible violations regarding Bioventus' compliance with this Privacy Program.

References

1. Information Security Policy (POL-000035)
2. Information Classification Policy (POL-000037)
3. The Bioventus Global Privacy Program (POL-000063)
4. Security Policy Review Checklist (POL-000034)

Review & Maintenance

This policy will be reviewed at planned intervals per the Security Policy Review Checklist (POL-000034) to ensure it remains valid and appropriate following any changes to applicable law, relevant international standards, organization policies, or contractual obligations. Review and any updates should also consider the general security climate, new and emerging threats, changes in the business, and changes in the industry best practice.

Policy Owner & Approvals

See SmartSolve for Policy Owner & Approvals