

IT Policy and Procedure

AI Acceptable Use Policy	SmartSolve #	POL-000091 [B]
	Page:	Page 1 of 8

Purpose

This Policy establishes requirements for the approved, responsible, ethical, secure, and legally compliant use of artificial intelligence (AI) at Bioventus.

Bioventus recognizes that AI can improve productivity, accelerate innovation, and enhance business outcomes. AI also introduces risks related to data protection, privacy, intellectual property, regulatory compliance, cybersecurity, transparency, reliability, and decision-making.

This Policy is intended to ensure that AI technologies are used consistently with Bioventus' values, risk-based governance approach, contractual commitments, regulatory obligations, and information security requirements.

Scope

This Policy applies to all Bioventus employees and non-employees, including contractors, consultants, temporary personnel, third parties, and guests, who access, store, process, manage, or otherwise interact with Bioventus systems, applications, networks, data, or information assets while using AI technologies. It applies to AI used on company-managed or personal devices for Bioventus business, including:

- Generative AI systems and large language models (LLMs)
- Agentic AI systems and autonomous or semi-autonomous agents
- Machine learning and predictive or analytical models
- AI-enabled software, cloud services, and SaaS platforms
- AI features embedded within approved applications
- Internally developed or configured AI solutions
- Third-party AI services, plugins, extensions, and integrations
- AI-generated or AI-assisted content, code, analysis, recommendations, and decisions

Definitions

Artificial Intelligence (AI): Technology that performs tasks commonly associated with human intelligence, including generating content, identifying patterns, making predictions, recommending actions, or executing defined activities.

AI Committee: The Bioventus governance body authorized to review and approve AI and AI-related use cases, including the approved use case, users, data types, risks, controls, and conditions of use.

Architecture Review Board (ARB): The Bioventus governance body responsible for reviewing new technology requests, including AI capabilities, for alignment with architecture, security, integration, supportability, and lifecycle requirements.

AI Agent: An AI capability that can plan or initiate actions, execute workflows, interact with systems, or use tools with some level of autonomy.



IT Policy and Procedure

AI Acceptable Use Policy	SmartSolve #	POL-000091 [B]
	Page:	Page 2 of 8

AI Drift: Changes over time in AI output, behavior, accuracy, consistency, or reliability caused by changes in models, data, prompts, vendor settings, configurations, or operating conditions.

AI-Enabled Software: Software, applications, systems, platforms, or services that include AI functionality, whether embedded, optional, or provided through a related feature, plugin, extension, integration, or third-party service.

AI-Generated Content: Text, images, audio, video, code, analysis, recommendations, summaries, or other outputs created or materially assisted by AI.

Bioventus Information: Information that Bioventus collects, creates, 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.

Electronic Protected Health Information (ePHI): Protected Health Information that is created, received, maintained, or transmitted electronically, including PHI stored in systems, applications, databases, files, emails, devices, cloud services, or other electronic media.

Generative AI: AI technology that creates new content or outputs, such as text, images, audio, video, code, summaries, analyses, or recommendations, based on user prompts or other inputs.

Large Language Model (LLM): A type of AI model trained on large volumes of text that can understand, generate, summarize, translate, or analyze language-based content.

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.

Third-Party AI: An AI platform, service, feature, model, or capability provided, hosted, or operated by a non-Bioventus party.

Guiding Principles

Business Value

AI shall support legitimate and approved business objectives and should create measurable organizational value.

Human Accountability

People remain accountable for decisions, actions, communications, and work products assisted by AI.

IT Policy and Procedure

AI Acceptable Use Policy	SmartSolve #	POL-000091 [B]
	Page:	Page 3 of 8

Security and Privacy

AI use must protect Bioventus information, intellectual property, personal information, and regulated data.

Transparency

AI involvement must be disclosed when appropriate, and AI-generated work must not be represented as validated or authoritative without review.

Regulatory Compliance

AI use must comply with applicable laws, regulations, contracts, and Bioventus policies.

Ethical Use

AI shall not be used in a deceptive, discriminatory, unlawful, unsafe, or harmful manner.

Approved Use

Authorized users may use approved AI capabilities for legitimate Bioventus business purposes, subject to the approved use case, data types, user population, and conditions of use. Examples may include:

- Research and information gathering
- Drafting and editing documents, emails, policies, and presentations
- Summarizing information
- Creating business content
- Analyzing approved data
- Assisting with software development
- Supporting approved process automation
- Reporting and productivity enhancement

Important

Approval of an AI tool does not mean every use case, data type, integration, or autonomous action is approved. Users must remain within the scope and conditions of the applicable approval.

Prohibited Use

- **Unapproved AI:** Using AI tools, agents, plugins, extensions, models, or services that have not been approved for Bioventus business use.

IT Policy and Procedure

AI Acceptable Use Policy	SmartSolve #	POL-000091 [B]
	Page:	Page 4 of 8

- **Restricted Data Submission:** Entering, uploading, exposing, or otherwise providing non-public, confidential, proprietary, personal, or regulated information to an AI system that has not been explicitly approved for that information.
- **Control Circumvention:** Using AI to bypass legal, regulatory, quality, security, privacy, procurement, records management, or governance requirements.
- **Unapproved Autonomous Decisions:** Allowing AI to make final legal, compliance, regulatory, quality, privacy, patient-care, financial reporting, employment, or other high-impact decisions without required human review and authorization.
- **Misrepresentation:** Representing AI-generated information as factual, validated, approved, original, or authoritative without appropriate verification or disclosure.
- **Malicious or Harmful Activity:** Using AI to create malicious code, fraudulent communications, deceptive content, harassment, unsafe instructions, or other content or actions that violate law or Bioventus policy.
- **Unauthorized Integration:** Connecting an AI capability to Bioventus systems, applications, identities, data sources, or workflows without required technical and governance approvals.

Data Protection Requirements

Data Classification and Use

AI use must comply with Bioventus data classification, privacy, security, records management, and data governance requirements. Public information may be used within approved AI tools. Non-public information may be used only where the AI environment and specific use have been approved for the applicable data classification.

The following information must not be entered into an AI system unless the system and use case have been explicitly approved for that information:

- Protected Health Information (PHI) or electronic PHI (ePHI)
- Personally Identifiable Information (PII) and employee records
- Confidential business information and trade secrets
- Financial reporting or SOX-relevant information
- Patient, clinical, quality, product safety, or regulatory submission data
- Source code, credentials, secrets, security configurations, or vulnerability information
- Contract information, legal advice, privileged information, or third-party confidential information

PHI and ePHI

No AI system may create, receive, maintain, or transmit PHI or ePHI on behalf of Bioventus unless IT Security, Compliance, Legal, and Privacy, as applicable, have approved the system and use, and Legal has executed any required Business Associate Agreement with the vendor. Consumer or free-tier AI services must never be used with PHI or ePHI.

IT Policy and Procedure

AI Acceptable Use Policy	SmartSolve #	POL-000091 [B]
	Page:	Page 5 of 8

Derived Outputs

AI-generated outputs derived from Bioventus data must be protected according to the sensitivity and classification of the source information and the content of the output.

Human Review and Validation

AI outputs may be inaccurate, incomplete, biased, outdated, inconsistent, or fabricated. Before relying on or distributing AI-assisted work, users must:

- Review the output for accuracy, completeness, appropriateness, and context
- Validate material factual statements, calculations, analyses, citations, and recommendations
- Confirm that the output complies with applicable policies, contracts, laws, and regulatory requirements
- Assess potential bias, unfairness, or inappropriate assumptions
- Obtain required subject matter, quality, legal, privacy, compliance, or management review
- Protect confidential information contained in prompts and outputs
- Apply professional judgment and remain accountable for the final work product

AI Governance and Approval

New AI tools, features, models, use cases, integrations, and agents must be submitted through applicable Bioventus governance processes before use or deployment.

AI Committee Review

The AI Committee must review the proposed business purpose, users, data classifications, legal and regulatory considerations, privacy impacts, security risks, vendor risk, human oversight, monitoring, and conditions of use.

Architecture Review Board Review

The ARB must review architecture, integrations, identity and access, security design, supportability, scalability, monitoring, change management, and lifecycle requirements.

Separate Approvals

Approval to use an AI tool does not automatically approve an integration, a new category of data, a materially different use case, or autonomous execution. Separate or renewed approval may be required.

AI Agents and Autonomous Systems

AI agents capable of initiating actions, executing workflows, using tools, interacting with other systems, or operating with autonomy require enhanced review and controls. At a minimum, approved AI agents must:

- Have a documented business owner, technical owner, purpose, scope, and approved users
- Use least-privilege access and approved identities

IT Policy and Procedure

AI Acceptable Use Policy	SmartSolve #	POL-000091 [B]
	Page:	Page 6 of 8

- Operate only against approved systems and data sources
- Maintain appropriate logging, traceability, and auditability
- Include monitoring, human oversight, and a means to suspend or stop operation
- Be tested before deployment and after material changes
- Be reviewed for drift, unexpected behavior, control failures, and continued business need
- Not execute high-risk or irreversible actions without explicit authorization and appropriate safeguards

Intellectual Property and Content

AI-generated or AI-assisted content created for Bioventus business is a work product subject to applicable Bioventus confidentiality, intellectual property, legal review, and records management requirements.

Users must not:

- Upload Bioventus intellectual property or proprietary information to unauthorized AI services
- Use third-party copyrighted, licensed, or confidential content in violation of applicable rights or restrictions
- Assume that AI-generated content is original, non-infringing, or suitable for external use
- Train or fine-tune an external model using Bioventus information without explicit approval
- Publish or externally distribute material AI-generated content without appropriate review

Security, Monitoring, and Records

AI activity may be subject to security logging, monitoring, retention, audit, and compliance review, consistent with applicable law and Bioventus policy. Bioventus may restrict, suspend, or revoke access to AI capabilities when needed to protect the organization or address noncompliance.

Business records created or materially assisted by AI must be retained and managed according to applicable Bioventus records management requirements. Users must not rely on AI chat history as the sole repository for required business records.

Training and User Responsibilities

Before using AI for Bioventus business, users must complete required training and understand the approved scope and conditions of use. Users are responsible for:

- Using only approved AI capabilities
- Protecting Bioventus information and technology resources
- Following data handling, privacy, security, and records requirements
- Reporting suspected misuse, data exposure, security events, or unexpected AI behavior
- Seeking guidance when the intended use or data is not clearly approved

IT Policy and Procedure

AI Acceptable Use Policy	SmartSolve #	POL-000091 [B]
	Page:	Page 7 of 8

Incident Reporting

Users must promptly report suspected AI-related data exposure, privacy incidents, security events, inaccurate high-impact outputs, unauthorized access, harmful behavior, or policy violations through established Bioventus reporting channels. Users must preserve relevant prompts, outputs, logs, and other available evidence and must not attempt to conceal or independently resolve a material incident outside established processes.

Reports can be made by contacting the Service Desk via the [self-service portal](#), emailing it_support@bioventus.com, or calling 1-855-284-8457.

Exceptions

Exceptions to this Policy must be documented, supported by a business justification and risk assessment, and approved by the appropriate Bioventus stakeholders before the exception is used. Exceptions may be time-limited and subject to additional controls or monitoring.

Violations and Enforcement

Violations of this Policy may result in removal of AI access, disciplinary action up to and including termination of employment or contract, legal action, and regulatory or contractual reporting where required.

References

1. Information Security Policy (POL-000035)
2. Acceptable Use Policy (POL-000036)
3. Information Classification Policy (POL-000037)
4. The Bioventus Global Privacy Program (POL-000063)
5. Security Policy Review Checklist (POL-000034)
6. Security Incident Response Policy (POL-000062)
7. Software Development Lifecycle Policy (POL-000051)
8. HIPAA Security Rule, 45 CFR Part 164 Subparts C and E

Policy Administration

Information Technology owns this Policy in coordination with IT Security, Legal, Privacy, Compliance, Quality, and other stakeholders as applicable. The Policy will be reviewed periodically and updated when material legal, regulatory, risk, business, or technology changes occur.

IT Policy and Procedure

AI Acceptable Use Policy	SmartSolve #	POL-000091 [B]
	Page:	Page 8 of 8

Appendix A. Quick Decision Guide

Question	If Yes	Required Action
Is the AI tool or feature approved?	Proceed to the next question.	If no or uncertain, do not use it for Bioventus business; submit it for review.
Will non-public, personal, confidential, regulated, or proprietary data be used?	Confirm explicit approval for that data classification and use case.	If approval is absent or unclear, do not enter or expose the data.
Will the AI connect to a system, application, identity, or data source?	Confirm technical, security, and ARB approval.	Do not integrate solely because the tool itself is approved.
Will the AI take actions or execute a workflow?	Confirm agentic or automation approval, controls, monitoring, and human oversight.	Do not enable autonomous or high-risk actions without explicit approval.
Will the output influence a high-impact decision or external communication?	Perform validation and obtain required expert or functional review.	A human remains accountable for the final decision and work product.
Did an incident, unexpected behavior, or possible data exposure occur?	Stop use if appropriate and report promptly.	Preserve relevant prompts, outputs, and logs; follow established incident processes.