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

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

IT Policy and Procedure

Information Security Policy	SmartSolve #	POL-000035 [B]
	ISO Reference #	IT-POL-01
	Page:	1 of 7

Purpose

The purpose of this policy is to provide a security framework that will ensure the protection of Bioventus Information from unauthorized access, loss or damage while supporting the tenets of Confidentiality, Integrity, and Availability. Bioventus Information may be verbal, digital, and/or hardcopy, individually controlled or shared, stand-alone or networked, used for administration, research, teaching, or other purposes.

The following Information Security objectives guide the Bioventus Information Security Policies:

- Data Loss Prevention – Protect Bioventus' formation assets against theft, abuse or loss.
- Improved Security of System and Network Services – Ensure the protection of all Bioventus information systems (including but not limited to all computers, mobile devices, networking equipment, software and data) and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems.
- Security Awareness- Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.
- Security Incident Management – Help Bioventus recover its information assets in the event of a security incident, data breach, or catastrophic event.
- Motivate administrators and employees to maintain the responsibility for, ownership of and knowledge about information security, in order to minimize the risk of security incidents.
- Regulatory Compliance - Comply with regulatory and legislative requirements such as HIPAA and EU GDPR and relevant best-in-class industry standards. (such as NIST, ISO, etc.).

The Information Security Policy is a collection of separate documents, which provides an extensible framework that can be updated to meet the needs of our business and address the dynamic information technology security landscape. Standards and procedures related to this Information Security Policy are developed and published separately. Where local law is stricter or conflicts with this Information Security Policy, local law takes priority.

Scope

The Information Security Policy applies to:

- all Bioventus employees, contractors, third-parties and guests who use or have access to Bioventus Information via any means including but not limited to technology (IT) infrastructure, computer equipment, mobile devices and information including all third-party cloud computing IT solutions;
- any device, regardless of ownership and including equipment privately owned by employees, contractors and guests (i.e., laptops, tablets, smart phones, USB storage devices, etc.), but only with respect to ways in which they connect to or access Bioventus Information resources and activities they perform with those resources; and
- all information that is owned by or entrusted to Bioventus.

Information Security Policy	SmartSolve #	POL-000035 [B]
	ISO Reference #	IT-POL-01
	Page:	2 of 7

Responsibilities

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

- Understand the information classification levels defined by the Information Security Policy;
- As appropriate, classify the information for which one is responsible and access information only as needed to meet legitimate business needs per the Bioventus *Information Classification Policy and Global Privacy Program*;
- Understand that the Information Security Policy is comprised of a framework containing all IT Security policies, standards and procedures that support the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).

Definitions

Authorization: the function of establishing an individual's privilege levels to access and/or handle information.

Availability: ensuring that information is ready and suitable for use.

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.

Cloud computing: the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. This includes Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and datacenter hosting facilities.

Confidentiality: ensuring that information is kept in strict privacy.

General Data Protection Regulation (EU) 2016/679 (GDPR): A regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union.

HIPAA: the Health Insurance Portability and Accountability Act, a federal law passed in 1996, as amended, that affects the healthcare and insurance industries. A key goal of HIPAA is to protect the privacy and confidentiality of protected health information by setting and enforcing standards via the HIPAA Security Rule.

Integrity: ensuring the accuracy, completeness, and consistency of information.

Policies: specify the information security intentions of Bioventus, grant authority, define roles and responsibilities, and establish high-level requirements for protecting the company's information resources.

Procedures: a systematic set of interrelated steps, tasks, or activities to be accomplished in order to implement a policy or standard to ensure that security policies and standards are applied in a consistent and repeatable manner.

Protected Health Information: 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.

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

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

IT Policy and Procedure

Standards: define the mandatory settings, controls, and requirements that must be implemented to achieve policy objectives. Compliance with standards is measurable, allowing risks to be identified, quantified, and managed at various organizational levels within the company.

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

Policy

Bioventus appropriately secures its information from unauthorized access, loss or damage while supporting the open, information-sharing needs of our business culture. All Bioventus Information is classified, per the *Information Classification Policy (POL-000037),* into one of four levels based on its sensitivity and the risks associated with disclosure:

- Sensitive / Restricted (high risk level)
- Confidential (medium risk level)
- Internal (low risk level)
- Public (no risk)

Sensitive / Restricted: Information is classified as **Restricted** if it contains Social Security Numbers, bank account numbers, driver's license numbers, state identity card numbers, credit card numbers, protected health information (PHI), or EU GDPR sensitive personal data. The unauthorized disclosure, modification, destruction, or disruption of access to Restricted information can have a **severe or catastrophic adverse effect** on Bioventus and its relationship with the subject individuals and could possibly carry significant liability.

Confidential: Information is classified as **Confidential** if it falls outside the Restricted classification but is not intended to be shared freely within or outside Bioventus due to its sensitive nature or contractual or legal obligations. The unauthorized disclosure, modification, destruction, or disruption of access to Confidential information can have a **serious adverse effect** on Bioventus. Examples of Confidential information include all non-Restricted information contained in personnel files, misconduct and law enforcement investigation records, internal financial data or other material non-public corporate information.

Internal: Information is classified as **Internal** if it is intended to be made available to anyone inside of Bioventus. Internal information is unfit for public consumption where the unauthorized disclosure, modification, destruction, or disruption of access to Internal information can have a **limited adverse effect** on Bioventus. Examples of Internal include company policies, standards, procedures, and security awareness materials.

Public: Information is classified as **Public** if it is intended to be made available to anyone inside and outside of Bioventus. The disclosure, use, or destruction of Public information will have **no adverse effects** on Bioventus.

The classification level determines the security protections that must be used for the information. Further details for the protection, handling and classification of may be found in the Bioventus *Information Classification Policy*.

Information Security Policy	SmartSolve #	POL-000035 [B]
	ISO Reference #	IT-POL-01
	Page:	4 of 7

Framework

The framework provides the structure for the Bioventus IT Security Program. The framework includes detail appropriate for various audiences and allows document ownership and approval to match authority and knowledge. References to the 'Bioventus Information Security Policy' are inclusive of all the published policies, standards, and procedures.

The framework is established based on guidelines for mitigating cybersecurity risks. It is based on 5 core functions that are subdivided into 23 categories and 108 subcategories.

IDENTIFY (ID)	
Asset Management (ID.AM)	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
Business Environment (ID.BE)	The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
Governance (ID.GV)	The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
Risk Assessment (ID.RA)	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
Risk Management Strategy (ID.RM)	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
Supply Chain Risk Management (ID.SC)	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.

PROTECT (PR)	
Identity Management Authentication and Access Control (PR.AC)	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.
Awareness and Training (PR.AT)	The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.
Data Security (PR.DS)	Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
Information Protection Processes and Procedures (PR.IP)	Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
Maintenance (PR.MA)	Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.
Protective Technology (PR.PT)	Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

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

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

DETECT (DE)	
Anomalies and Events (DE.AE)	Anomalous activity is detected, and the potential impact of events is understood.
Security Continuous Monitoring (DE.CM)	The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Detection Processes (DE.DP)	Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.

RESPOND (RS)	
Response Planning (RS.RP)	Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.
Communications (RS.CO)	Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).
Analysis (RS.AN)	Analysis is conducted to ensure effective response and support recovery activities.
Mitigation (RS.MI)	Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.
Improvements (RS.IM)	Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

RECOVER (RC)	
Recovery Planning (RC.RP)	Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.
Improvements (RC.IM)	Recovery planning and processes are improved by incorporating lessons learned into future activities.
Communications (RC.CO)	Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).

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

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