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

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

IT Policy and Procedure

Information Technology Acceptable Use Policy	SmartSolve #	POL-000036
	ISO Reference #	IT-POL-03
	Page:	1 of 7

Purpose

This policy establishes specific requirements for the use of all computing, data, and network resources 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 these devices, services and facilities, you have access to valuable company resources, to sensitive personal data, and to internal and external networks. Consequently, it is important for you to behave in a responsible, ethical, and legal manner.

In general, acceptable use means respecting the rights of other computer users, the integrity of the physical facilities and managed services and all pertinent license and contractual agreements. If an individual is found to be in violation of this policy, Bioventus may take disciplinary action, including the restriction and possible loss of network privileges. Where local law is stricter or conflicts with this Policy, local law takes priority. In addition, this policy adheres to and supports the Bioventus *Global Privacy Program.*

Scope

The Acceptable Use 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.
- 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 Acceptable Use policy;
- Be responsible for the information resources provided to you by Bioventus;
- Control unauthorized use of your information resources by preventing others from obtaining access to your computer and mobile device;
- Safeguard your Bioventus credentials and not use easy-to-guess passwords;
- Exercise good judgement in the use of Bioventus' technological and information resources;
- Acknowledge Acceptable Use Examples.

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

- Ensure his/her employees understand and adhere to the 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

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

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

IT Policy and Procedure

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.

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 datacentre hosting facilities.

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.

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.

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

Policy

This policy establishes guidelines for acceptable use of information resources. It includes examples of what you can do and cannot do, and what rights you have. All of these guidelines are based on the following underlying principles:

- Information resources are provided to support the essential business functions of Bioventus
- Bioventus policies, state and federal law govern your use of information resources
- You are expected to use information resources with courtesy, respect, and integrity.
- The information resources infrastructure is provided for the company. This infrastructure is finite and requires resources to maintain, and all users are expected to use it responsibly.
- Simply because an action is easy to do technically does not mean it is legal or even appropriate.

See Acceptable Use Examples (Appendix 1) to clarify Bioventus' interpretation of acceptable use.

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 Security Policy (POL-000035)
3. Global Privacy Program

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

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

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

IT Policy and Procedure

Appendix 1: Acceptable Use Examples

Passwords

Acceptable:

- Use of a password manager application for storing *personal, non-Bioventus* passwords

Unacceptable:

- Giving your password to anyone – including Bioventus IT and the Service Desk.
- Storing your BV ID password in a password manager application
- Storing your BV ID password in a text file or Word document on your laptop
- Writing your BV ID password on anything in close proximity to your laptop or mobile device

eMail / ***Electronic Communication***

Acceptable:

- Electronic communications are formal business communications, and users are expected to exercise the same care and professionalism in creating messages as they would when speaking on the phone or writing a letter or memo on behalf of the company.
- Electronic communications should be used when documentation of communication is needed or when it is deemed more efficient and effective than a telephone call or other written communication.
- General standards for electronic communications include:
    - Using only company-authorized electronic communications systems when messages contain confidential or proprietary company information
    - Using an access facility approved by Information Security when using company electronic communications systems with a remote connection
    - Keeping messages as small in size as possible and limiting the distribution of messages that contain large attachments, graphics, or animation
    - Using electronic communications in an ethical and lawful manner. Being accountable for the information sent over electronic communications systems by using electronic communications professionally and appropriately
    - Using company electronic communications systems for company business (personal communications may be sent consistent with this policy as long as they do not interfere with normal business activities)
    - Protecting confidential and sensitive company and personal information in accordance with company's Information Classification policy and Global Privacy Program.
    - Preventing those outside the company from gaining access to company electronic communications resources except by prior approval of the Head of IT Security Operations.

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

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

IT Policy and Procedure

Unacceptable:

- Conducting personal business via Bioventus email
- Forwarding your Bioventus email to a non-Bioventus, personal email account
- Emailing credit card information to anyone for any reason
- Using personal email for submitting sales orders or sending Protected Health Information (PHI), etc.
- Using any electronic communications systems or tools not provided by the company to distribute, comment on, or share confidential or proprietary company information
- Using electronic communications resources to distribute information that is inconsistent with company policy, contrary to the company's interests, or violates law
- Information that is obtained or used for personal gain (e.g., non-company for-profit business affairs)
- Defamatory, discriminatory, abusive, sexually oriented, harassing, obscene, threatening, or otherwise inappropriate information
- Information that is rumor or embarrassing in nature
- Sarcastic or inappropriate humor
- Information or data of any type that violates another's rights in copyrighted or trademarked materials by downloading, sending, or copying materials, files, etc., in violation of the terms of usage or license
- Chain letters
- Information about business activities that can be transmitted or captured more effectively via transaction-oriented systems (e.g., information that is usually captured or saved in files or databases)
- Business information for which well-defined audit trails are required including non-company advertisements or solicitations
- Responding to unsolicited or junk electronic communications and spam broadcasting messages of a personal nature or offering items for sale
- Disguising one's identity in electronic communications
- Purposefully wasting company computing resources or monopolizing those resources, which includes sending unnecessary mass mailings, printing multiple copies of documents, and subscribing to non-business list servers (discussion groups conducted through e-mail)
- Using systems other than e-mail to communicate information that is privileged and confidential-violations of this policy may result in disciplinary action including termination of employment.

Computers (Laptops & Desktops)

Acceptable:

- Responsible and ethical personal internet browsing when not interfering with business responsibilities and activities
- Connect to known or reputable public wireless networks (e.g. airport, train, coffee shops, etc.) and then immediately connect the Cisco AnyConnect Secure Mobility Client (VPN)
- Storing business-critical files on Bioventus network (H:\, N:\ drives, etc.), OneDrive, SharePoint or other authorized systems.

Unacceptable:

- Connect to any public wireless networks *and not* connecting the Cisco AnyConnect Secure Mobility Client (VPN)
- When at the office, connecting your laptop to the PURPLE (guest) wireless network
- Allowing family or friends to use a Bioventus laptop
- Leaving laptop and any printed material unattended or in plain view in a vehicle, on public transit, at airport, on airplane, etc.
- Long-term storing of business-critical files on your laptop's physical disk (Desktop, Documents, etc.)
- Use of torrents and similar services to download illegal content to a Bioventus device

Fax

Acceptable

- Using Bioventus-approved electronic fax service: Concord Fax

Unacceptable

- Using a personal/at-home traditional fax machine instead of using Concord Fax
- Using unapproved electronic fax service: eFax, MetroFax, etc.

Cloud/Internet File Sharing

Acceptable:

- Using Bioventus-approved file sharing service: Microsoft OneDrive, SharePoint

Unacceptable:

- Using unapproved file sharing services without authorization from Compliance: Dropbox, WeTransfer, Box, Google Drive, etc.

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

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

IT Policy and Procedure

Mobile Devices

Acceptable:

- Responsible and ethical personal internet browsing when not interfering with business responsibilities and activities
- Using approved Photo-to-PDF apps: Adobe Acrobat, Scanner Pro
- Using approved mobile phone or tablet operating system: iOS
- When at a Bioventus office, connecting your mobile device to the PURPLE (guest) wireless network

Unacceptable:

- Using any unapproved mobile phone or tablet operating system: Android, Windows Phone, B&N Nook, Amazon Fire, Galaxy, etc.
- Charging a non-iOS (ex. Android) via USB cable connected to your Bioventus laptop

Data Access & Usage

Acceptable:

- Limit the collection of personal data, obtained by lawful and fair means, and where applicable, with the knowledge or consent of the data subject per EU GDPR
- Accessing, modifying, copying data based per the Bioventus Information Classification Policy and Global Privacy Program.
- With respect to the processing of sensitive personal data, some applicable laws (HIPAA & EU GDPR) require heightened privacy requirements.

Unacceptable:

- Looking up, reviewing, copying, modifying, deleting, analyzing, providing access, or handling information without proper authorization or legitimate business need
- Handling of data that violates the Bioventus Information Classification Policy or Global Privacy Program
- Failing to redact sensitive personal data and/or protected data prior to training / testing usage
- Including sensitive personal data / restricted data in testing documentation