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

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

IT Policy and Procedure

Electronic Communications Security Policy	SmartSolve #	POL-000050 [B]
	Governance Ref #	IT-POL-GOV-14
	Page:	1 of 6

Purpose

The purpose of the electronic communications policy is to:

- Ensure employees and contractors follow the appropriate guidelines when using all forms of electronic communication according to the standards set by Bioventus
- Ensure use of electronic communications systems primarily for business-related purposes
- Prevent the unauthorized or inadvertent disclosure of sensitive personal data or corporate information, protected personal or health information
- Limit the possibility of damage and unauthorized company systems and data.

Corporate electronic communications, including, but not limited to, email services, instant messages, social media, file sharing, fax services, etc are provided to serve operational and administrative purposes in connection with the business.

All electronic communication processed by the corporate IT systems and networks, including cloud services, are considered to be the organization's property.

Scope

This policy applies to all employees, contractors, consultants, temporary staff, and third-party contractors. This policy supports all regulatory rulings (i.e. HIPAA & EU GDPR) and the Bioventus Global Privacy Program and applies to all electronic communication resources, including, but not limited to company's network, computers, workstations, laptops, tablets, software, hardware, internet / intranet, email, fax machines / fax services, voice-mail, telephones and mobile phones.

This application security policy represents the minimum standard. Where local law is stricter or conflicts with these policies, local law takes priority.

Responsibilities

All Bioventus employees and third party employees acting in a similar capacity, are responsible for the following:

- Understand and adhere to the Electronic Communications Security Policy
- Report any known abuse or violation of this policy to IT Head of Security

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

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

IT Policy and Procedure

Definitions

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

***Chain Letter*:** E-mail sent to successive people; typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed

Confidentiality: ensuring that information is kept in strict privacy.

E-mail: The electronic transmission of information through a mail protocol such as SMTP or IMAP

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.

Electronic Communications System: Voice-mail, e-mail, intranet, or Internet access system owned, leased, operated, maintained or managed by the company.

Forwarded E-mail: E-mail resent from an internal network to an outside point

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.

Messages: All messages, files, or other data created, uploaded, downloaded, sent, received, or stored on any electronic communications system.

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.

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.

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

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

IT Policy and Procedure

Electronic Communications Security Policy	SmartSolve #	POL-000050 [B]
	Governance Ref #	IT-POL-GOV-14
	Page:	3 of 6

Policy

Right to Access / Privacy

1. Electronic information resources, telephonic communication systems, and all data residing therein belong to Bioventus and may be viewed or accessed at any time without consent or knowledge of the sender or receiver, as approved / requested by HR, Legal and/or Compliance.
2. Limited non-business use of company's electronic information resources and telephonic communication systems is permitted, however, it is understood that employees have limited privacy expectations in any electronic information resources, telephonic communication systems, or data therein.
3. The company reserves the right to monitor, access, and review any aspects of its electronic information resources and telephonic communication systems, including but not limited to, monitoring Internet use, reviewing e-mail sent and received by employees, sniffing network traffic, and reviewing files stored on any communication system.

Provision on Recording Telephone Conversations

1. To the extent authorized by applicable federal, state, or local laws, the company may record certain telephone conversations.
2. The purpose of such recording is usually to provide verification of transactions entered into by the company on its own behalf and on behalf of its customers, to protect the organization against employee misconduct, and to ensure the telephone lines are being used consistent with applicable company policies.
3. Employee's consent to such recording and monitoring is presumed by employee's use of company phone lines.

E-mail

1. All e-mail should be retained / deleted per the corporate Records Retention Policy (GPP24: Records Retention) located on Bionet.
2. Do not use your Bioventus email to sign-up for personal services (i.e. shopping, coupons, memberships, file sharing)
3. Employees will strive to keep a majority of his or her e-mails related to business issues.

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

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

IT Policy and Procedure

Personal Use

1. All electronic information resources and telephonic communication systems are the property of the company and should be used primarily for company business purposes.
2. Limited non-business use of electronic information resources and telephonic communication systems may be permitted if the use does not:
    1. Interfere with the employee's work performance;
    2. Interfere with any other employee's work performance;
    3. Have undue impact on the operation of the electronic information resource or communication system; and
    4. Violate any other provision of this policy, the Code of Conduct, the Bioventus Global Privacy Program, or any other policy, guideline, or standard of the company.

Confidential Information Security

1. The company has an obligation to maintain the confidentiality of its own information and information of third parties that may be communicated through the company's electronic communications system.
2. All users of the company electronic communications system must take steps to ensure the security of the system and to maintain the confidentiality of all e-mail and other information on the system or communicated through the use of the company electronic communications system.
3. Information should be classified and managed according to company's information classification policy.

USB / Removable Storage

1. The company has an obligation to maintain the confidentiality of its own information and information of third parties that may be communicated via the use of removable storage

2. As such, Bioventus requires the use of encryption for all removable storage devices connecting to Bioventus equipment in order to write to these devices.

3. Bioventus IT Security will review exception requests to this policy as submitted to the Help Desk, within 24 hours, and will approve / deny based on security risk assessment.

4. Employees are not to use personal devices to circumvent this policy.

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

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

IT Policy and Procedure

Passwords

1. It is prohibited to share your password / credentials with anyone.
2. Employees are responsible for activities carried out by others, if password / credentials are shared.

Retention and Litigation

1. Company employees should be aware that communications can be retained on the system, and, even if no longer retained on the user's machine, they may be retained by the recipients or forwarded to others whom the user never intended to receive them.
2. Electronic communications are discoverable and subject to subpoena by outside persons and entities in arbitration/litigation and regulatory proceedings.

Instant Messages

1. Teams is the only Instant Messaging software that is approved for use on company computers.
2. General correspondence on the company Team system will be saved with the logging function built into the platform.

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.

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

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

IT Policy and Procedure

References

1. Security Policy Review Checklist (POL-000034)
2. IT Acceptable Use Policy (POL-000036)
3. Information Classification Policy (POL-000037)
4. Information Security Awareness Policy (POL-000038)
5. The Bioventus Global Privacy Program (POL-000063)
6. General Data Protection Regulation (EU) 2016/6790 (GDPR)
7. Records Retention Policy (GPP24)

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