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

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

IT Policy and Procedure

System Usage Monitoring Policy	SmartSolve #	POL-000061[B]
	Governance Ref #	IT-POL-GOV-20
	Page:	1 of 4

Purpose

The purpose of this policy is to enable Bioventus to:

- Define standards for systems that monitor and limit web use from any host within the Bioventus network;
- Ensure employees use the Internet in a safe and responsible manner; and
- Ensure that employee web use can be monitored or researched during an incident

Scope

The System Usage Monitoring Policy applies to all Bioventus employees, contractors, third-parties and guests who use the internet and web and connect to the Bioventus network.

Responsibilities

It is the responsibility of all company employees to ensure that company systems are used only for fulfilling the company business requirements and to comply with the IT Acceptable Use Policy (POL-000036).

The information security officer will periodically review system use monitoring and filtering systems and processes to ensure they are in compliance with this policy.

The company reserves the right to inspect an employee's computer system for violations of this policy.

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 datacentre 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.

Hacking: Sites that provide content about breaking or subverting computer security controls.

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.

System Usage Monitoring Policy	SmartSolve #	POL-000061[B]
	Governance Ref #	IT-POL-GOV-20
	Page:	2 of 4

Internet Filtering: Technology that monitors each instance of communication between devices on the corporate network and the Internet and blocks traffic that matches specific rules

IP Address: Unique network address assigned to each device to allow it to communicate with other devices on the network or Internet

OpenAI: American artificial intelligence (AI) research organization founded in December 2015, researching artificial intelligence with the goal of developing "safe and beneficial" artificial general intelligence, which it defines as "highly autonomous systems that outperform humans at most economically valuable work".

Peer-to-Peer (P2P) File Sharing: Services or protocols such as BitTorrent that allow Internet connected hosts to make files available to or download files from other hosts.

Phishing: Attempting to fraudulently acquire sensitive personal information by masquerading as a trusted entity in an electronic communication.

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.

SMTP: Simple Mail Transfer Protocol. The Internet Protocol that facilitates the exchange of mail messages between Internet mail servers

Social Networking Services: Internet sites such as Google+ and Facebook that allow users to post content, chat, and interact in online communities.

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

Network Traffic / Communications Monitoring

- IT and IT Security has the right to monitor network and Internet use from all computers and devices connected to the corporate network.
- For all traffic monitored, the monitoring system may record the source IP Address, the date, the time, the protocol, and the destination site or server. Where possible, the system should record the user ID of the person or account initiating the traffic.

Access to Website Monitoring Reports

System Usage Monitoring Policy	SmartSolve #	POL-000061[B]
	Governance Ref #	IT-POL-GOV-20
	Page:	3 of 4

- Internet use reports that identify specific users, sites, teams, or devices will only be made available to associates outside the incident response team upon written or e-mail request to information systems from Human Resources, Legal or Compliance representative.
- Incident response team members may access all reports and data, if necessary, to respond to a security incident.

Internet Use Filtering

IT Security may block access to Internet websites and protocols that are deemed inappropriate or risky for Bioventus' corporate environment. The following categories, include but are not limited to, websites that may be blocked:

- Malware
- Personal VPN tunnels
- Explicit Material
- Advertisements and Pop-Ups
- Gambling
- Hacking
- Illegal Drugs
- Peer-to-Peer (P2P) File Sharing
- Personals and Dating
- Tasteless and Offensive Content
- Violence, Intolerance, and Hate
- Chat and Instant Messaging
- Social Network Services
- OpenAI

Employees shall not place company material (copyrighted software, internal correspondence, etc.) on any publicly accessible Internet computer without prior permission. Alternate Internet Service Provider connections to company's internal network are not permitted unless expressly authorized and properly protected by a firewall or other appropriate security device(s). Files that are downloaded from the Internet must be scanned with virus detection software before installation or execution. All appropriate precautions should be taken to detect for a virus and, if necessary, to prevent its spread.

Internet Use Filtering Rule Changes

- The IT department shall periodically review and recommend changes to web and protocol filtering rules. Human Resources may review these recommendations and decide if any changes are to be made.

Internet Use Filtering Exceptions

- If a site is improperly categorized, employees may request the site be unblocked by submitting a ticket to the IT help desk or IT Security.
- An IT Security employee will review the request and unblock the site if it is improperly categorized.
- Employees may access blocked sites with permission if appropriate and necessary for business purposes.
- If an employee needs access to a site that is blocked and appropriately categorized, he or she must submit a request to the IT help desk or IT Security.

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

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

IT Policy and Procedure

- IT Security will review and approve / deny requests to the filtering exceptions as submitted to the IT Help Desk, within 24 hours, and will approve / deny based on security risk assessment.
- IT Security will track approved exceptions and report on them upon request.

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. 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)

Review & Maintenance

This policy will be reviewed regularly at planned intervals per the Security Policy Review Checklist (POL-000034) to ensure it remains 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