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

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

IT Policy and Procedure

Mobile Device Security Policy	SmartSolve #	POL-000059 [B]
	Governance Ref #	IT-POL-GOV-018b
	Page:	1 of 5

Purpose

The purpose of this policy is to ensure

- That all Bioventus employees are aware of their individual responsibilities in relation to the use of corporate-provisioned or personal mobile computing devices for the recording and storing of sensitive personal or corporate information and for access to the Bioventus systems.
- That all Bioventus employees who work remotely are aware of the acceptable use of portable computer devices and remote working opportunities.
- Mobile computing device policy and usage of devices by employees supports to Bioventus Global Privacy Program and all regulatory rulings around protected health information (PHI) and personal identifying information (i.e. HIPAA & EU GDPR).

Scope

This policy applies to

- All employees of Bioventus, including part-time employees, temporary hires (interns, and contractors), and third parties that have access to Bioventus Information assets.
- Devices that can be used as part of teleworking or mobile working include:- PCs (home based), laptops and notebooks, tablets, smart phones, mobile phones and any other mobile device that records and/or processes information.

This security policy represents the minimum standard.

Where local law is stricter or conflicts with these policies, local law takes priority.

Mobile Device Security Policy	SmartSolve #	POL-000059 [B]
	Governance Ref #	IT-POL-GOV-018b
	Page:	2 of 5

Responsibilities

It is the responsibility of all employees:

- To ensure they are familiar with the content of this policy
- To comply with all conditions contained within this document, for example regarding confidentiality, remote working, data protection, acceptable use, etc.
- To speak to their manager for any advice or clarification
- To immediately report any loss, theft or damage to a mobile device Bioventus owned or personally owned used to conduct Bioventus business, in the event of data breach

It is the responsibility of the Director of IT Security, Risk & Compliance for the overall enforcement of the policy.

- Ensuring that all provisioned devices are appropriately secured
- Reviewing the arrangements for remote workers with Human Resources on a regular basis
- Monitoring the use of Bioventus mobile computing devices and ensuring compliance with this Policy

It is the responsibility of Bioventus Managers for:

- The approval for remote working in line with the guidance provided in this policy
- Reviewing any existing remote working arrangements for staff within their area of responsibility in line with the guidance contained within this policy
- Ensuring that all staff utilizing mobile computing devices within their area of responsibility understand this policy and have sufficient knowledge concerning the security of information and systems
- Collecting and returning to IT, within 7 days of termination, all mobile computing devices purchased by Bioventus.

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.

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.

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.

Head of Information Technology Security: Information Security Officer

Mobile Computing Device: Mobile computing devices are handheld devices (phones, tablets, laptops, etc) that have the hardware and software required to execute typical desktop and Web applications. They have similar hardware and software components as those used in personal computers, such as processors, random memory and storage, Wi-Fi, and a base operating system. However, they differ from PCs in that they are built specifically for mobile architecture and to enable portability.

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.

Proprietary Information*:* Nonpublic information generated by or entrusted to the organization.

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.

Public Information: Information that has been made available to the public domain through authorized company channels and requires no special protection.

Remote Working: Remote working is used to describe the act of working from a location other than the traditional office. It is often used interchangeably with telecommuting and includes resources work remote on a regular or intermittent basis.

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

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

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

IT Policy and Procedure

Mobile Device Security Policy	SmartSolve #	POL-000059 [B]
	Governance Ref #	IT-POL-GOV-018b
	Page:	4 of 5

Policy

Appropriate measures must be taken when using mobile devices to ensure the confidentiality, integrity and availability of sensitive information, including protected health information (PHI) and sensitive personal information (per EU GDPR). All mobile devices accessing the corporate network must have the Bioventus approved mobile device management (MDM) software client installed. The client will enforce the following security measures:

Employee Responsibilities:

1. The employee can connect Bioventus provisioned devices to the personal/home broadband network for work purposes. Where connection is Wireless, users MUST ensure that the wireless connection security is enabled to at least WPA WPA2 or equivalent authentication.
2. To ensure confidentiality of business information, unauthorized individuals, including family members, should not be allowed to access company-provisioned devices.
3. When using wifi, consider the following from most secure to lease secure:
   - Personal mobile device tether that uses mobile phone network.
   - Use only a trusted source (i.e. official airport wifi, business wireless)
   - Never use an unknown wifi or personal hotspot
4. If connecting to public wifi from a personal device, ensure that device is kept up to date with patches and system updates.
5. Employees should report all incidents that constitute a loss of equipment or data, which could potentially lead to a data breach, directly to IT Service Desk @ 855-284-8457. The IT Security team will initiate investigation procedures where required and establish the nature and potential threat of the incident. See the IT Incident Response Policy (POL-000062) for details.

   a) Incidents could involve:
      - Loss of Hardware
      - Loss of Software/Data Virus attack
      - Unauthorized access Misuse of System/Privileges Illegal software download

IT Responsibilities

1. Only approved mobile device platforms may access Bioventus information;
2. Mobile devices must be password enabled. Access to the device must be restricted only via typing the correct password;
3. A mobile device password must be a minimum of four characters and/or numeric digits.
4. A mobile device must be able to encrypt its data upon Bioventus mobile device management approval.
5. The mobile device must be configured to lock after 10 unsuccessful passwords attempts to access the device;
6. Mobile devices must have password protected screen savers enabled. The password protected screen saver must be enabled after 10 minutes of inactivity;
7. If the mobile device is lost or stolen, all Bioventus data must be remotely wiped from the device, if possible;
8. The approved MDM software must be able to detect when a mobile device has been jail broken and/or rooted;

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

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

IT Policy and Procedure

Mobile Device Security Policy	SmartSolve #	POL-000059 [B]
	Governance Ref #	IT-POL-GOV-018b
	Page:	5 of 5

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. IT Acceptable Use Policy (POL-000036)
4. Information Classification Policy (POL-000037)
5. Information Security Awareness Policy (POL-000038)
6. Electronic Communication Security Policy (POL-000050)
7. IT Password Policy (POL-000056)
8. IT Security Incident Response Policy (POL-000062)
9. The Bioventus Global Privacy Program (POL-000063)
10. Global T&E Policy – Mobile Device Section (GPP23)

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