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

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

IT Policy and Procedure

IT Password Policy	SmartSolve #	POL-000056 [B]
	Governance Ref #	IT-POL-GOV-17c
	Page:	1 of 4

Purpose

Passwords - the front line of protection for user accounts - are an important aspect of computer security. A poorly chosen and managed password may result in the compromise of the Bioventus corporate network. As such, all Bioventus employees and contractors (including administrators, contractors and vendors with access to the Bioventus information systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Scope

The scope of this policy includes all employees and contractors who have or are responsible for an account on the Bioventus information system(s). This policy must be implemented in the following types of information system accounts:

- All information systems user accounts
- All information system infrastructure and application administration accounts

This policy represents the minimum standard.

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

Responsibilities

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

- Understand and comply with the IT Password Policy;
- Be responsible for protecting your ID and password and never
  - Provide it to anyone for any reason
  - Store a password in a written format
  - Keep it in an application (i.e. MS Outlook, MS Excel, MS Word, etc)
  - Store it in a non-approved password keeper
- 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;

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

- Ensure his/her employees understand and adhere to the IT Password Policy
- Understand the policy and address adherence issues of his/her employees through additional training
- Report violations of IT Password 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

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.

Passphrases: A longer version of a password, a passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against dictionary attacks.

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.

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.

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

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

IT Policy and Procedure

IT Password Policy	SmartSolve #	POL-000056 [B]
	Governance Ref #	IT-POL-GOV-17c
	Page:	3 of 4

Policy

Domain User Accounts

All bv.corp Domain User account passwords (i.e., our BV ID password) must meet the following minimum requirements:

- *Minimum Password Length:* A passphrase consisting of a minimum of 15 characters
- *Password Must Meet Complexity Requirements:* False
- *Maximum Password Age:* 365 days
- *Enforce Password History:* 24 password remembered
- *Account Lockout Threshold:* 5 invalid attempts

Other

Application or device-specific passwords that are not able to meet the minimum requirements of the Domain User accounts Password Policy are acceptable provided that they meet the following specification:

- *Minimum Password Length:* A passphrase consisting of a minimum of 8 characters
- *Password Must Meet Complexity Requirements:* True
- *Maximum Password Age:* Configurable
- *Enforce Password History:* Configurable
- *Account Lockout Threshold:* Configurable

Any system being considered for deployment at Bioventus that is not able to comply with the requirements set forth in this policy must be evaluated by a risk assessment conducted by Information Security.

Password Reset Guidelines

- All password resets must be documented in either the Bioventus IT Service Desk ticketing system, system event logs or in written documentation.
- The list of IT administrators having the privilege to reset passwords must be maintained and reviewed once per year.
- The Bioventus IT Service Desk must correctly identify the employee requesting a password reset by asking the employee to verify their BV ID and Manager's Name.
- Once the employee's identity has been verified, the Bioventus IT Service Desk will reset the password and force the user to change it upon next login.

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-000036)
3. Information Classification Policy (POL-000037)
4. Information Security Awareness Policy (POL-000038)
5. SAP Emergency Repair (Firefighter) Usage Policy (POL-000041)
6. Network Security Policy (POL-000049)
7. Database Security Policy (POL-000053)
8. IT Account Management & Resource Policy (POL-000054)
9. IT Admin Account Management Policy (POL-000055)
10. 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