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

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

IT Policy and Procedure

End User SAP Access Policy	SmartSolve #	POL-000057
	Governance Ref #	IT-POL-GOV-17d
	Page:	1 of 3

Purpose

This is the Bioventus Information Technology (IT) End User SAP Access policy to ensure that access to Bioventus Information created and maintained in our Enterprise Resource Planning (ERP) system, SAP, is appropriate based on the individual's role and responsibilities within the company.

Scope

This policy applies to all Bioventus departments, employees, contractors requiring Bioventus SAP Access, including permanent / on-going roles as well as Emergency / Firefighter access (see SAP Emergency Repair (Firefighter) Usage Policy (POL-000041), to perform their job functions.

This policy represents the minimum standard.

Where local law is stricter or conflicts with this policy, local law takes priority.

Responsibilities

The Bioventus Functional Business owner or Employee's manager

- Will request access authorization for end users to the SAP system.
- Is responsible for training and/or providing user guides to employee requesting SAP access

The Bioventus IT SAP Security Administrator will be responsible for:

- Verifying segregation of duties within requested roles/transaction, identifying potential conflicts, and working with internal audit to resolve segregation of duties conflicts by the use of current mitigations or blocking the requested SAP Access
- Providing the requested access to the SAP system.

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.

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.

SOD: Segregation of Duties is a security concept to prevent potential fraud by reducing or eliminating conflicting roles / transactions that may allow for fraud activities.

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

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

IT Policy and Procedure

End User SAP Access Policy	SmartSolve #	POL-000057
	Governance Ref #	IT-POL-GOV-17d
	Page:	2 of 3

Policy

1. No user shall log in to SAP with any User ID / password other than their own
2. No user shall provide their SAP User ID / password to any other user for any reason
3. Do not write down your SAP User ID / password
4. If it is determined that a Bioventus end user requires access to the SAP system for business purposes, the end user or end user's functional manager will be responsible for submitting the Global SAP security access form to the IT security team;
5. Once completed, if required, approval will be required from the SAP Role approver. In most instances this will be the same person as the functional manager;
6. No violations of Segregation of Duties, unless mitigated, shall be granted, regardless of user requesting;
7. No assignment of sensitive TCODES (eg. SE16) shall be granted for any reason.
8. No SAP_ALL or equivalent role requests shall be fulfilled
9. Approval from the Bioventus IT SAP Security team will be required for ALL SAP resource access requests;
10. If, after checking the new access / role requested for sensitive access / TCODES and the absence of Segregation of Duty violations, the Bioventus IT SAP security team shall approves the access, the access request will be forwarded to the Bioventus IT SAP administrator. The SAP administrator will grant the access as per the Global SAP security access form.

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 Awareness Policy (POL-000038)
3. SAP Emergency Repair (Firefighter) Usage Policy (POL-000041)
4. SAP Global Security Access Request Form (located on Bionet)
5. SAP Global Security Access Request Guide (located on Bionet)

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.

End User SAP Access Policy	SmartSolve #	POL-000057
	Governance Ref #	IT-POL-GOV-17d
	Page:	3 of 3

Policy Owner & Approvals

See SmartSolve for Policy Owner & Approvals