 SOUTHEAST MISSOURI STATE UNIVERSITY · 1873	BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 10/23	Revision Date:	Page: 1 of 3
				Classification Code: 10-17
		Section: INFORMATION TECHNOLOGY		
		Subject: GENERIC ACCOUNT POLICY		

PURPOSE:

The Generic Account Policy at Southeast Missouri State University is established to provide a robust framework for creating, utilizing, and maintaining generic accounts. This policy is crucial to ensure the security and manageability of our Active Directory (AD) infrastructure. Generic accounts, associated with functions, roles, or groups rather than specific individuals, play a pivotal role in supporting various operational and business needs across the University. However, the inherent risks associated with these accounts necessitate a comprehensive policy that governs their creation, access, and ongoing management.

The aims of this policy are to:


1. **Mitigate Security Risks:** If not properly managed, generic accounts pose security risks such as unauthorized access and misuse. This policy establishes guidelines for creating strong passwords, implementing access controls, and regularly monitoring account usage to safeguard against potential threats.
2. **Ensure Accountability and Compliance:** The policy outlines a straightforward approval process for creating generic accounts and responsibilities for the AD Administration Authority and all University stakeholders. This policy fosters accountability and ensures compliance with the established guidelines.
3. **Promote Efficient Use of Resources:** Periodic reviews and documentation requirements outlined in the policy contribute to the efficient use of University resources. By regularly assessing the necessity of generic accounts, we prevent the proliferation of unnecessary accounts and maintain a streamlined and secure AD infrastructure.
4. **Facilitate Auditing and Reporting:** The policy mandates the logging and monitoring of generic account usage, providing a means to track and report any unauthorized access or misuse. This proactive approach enhances the University's ability to promptly identify and address potential security incidents.
5. **Support a Culture of Security Awareness:** Training and awareness initiatives outlined in the policy contribute to fostering a culture of security among users. Ensuring that individuals granted access to generic accounts are informed about responsible usage practices further strengthens the University's overall cybersecurity posture.

POLICY SCOPE:

This policy applies to all departments, employees, contractors, and other stakeholders involved in the management and use of University generic accounts.

DEFINITIONS

Active Directory (AD): A Microsoft product that consists of services that help administrators manage users and resources in a network.

 SOUTHEAST MISSOURI STATE UNIVERSITY · 1873	BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 10/23	Revision Date:	Page: 2 of 3	
				Classification Code: 10-17	
		Section: INFORMATION TECHNOLOGY			
		Subject: GENERIC ACCOUNT POLICY			

Generic Account: An account not associated with a specific individual but with a function, role, or group of individuals.

POLICY STATEMENT

This policy applies to all University generic accounts and mandates the following:

Creation of Generic Accounts:

- Generic accounts must only be created to fulfill legitimate University operational or business needs.
- Southeast Missouri State University Information Technology retains the power to determine how, when and if a generic account is created.
- A formal request for the creation of a generic account must be submitted detailing the purpose, the individuals or groups who will have access, and the duration for which the account is required.

Naming Convention:

- Generic accounts should adhere to a standardized naming convention to be developed and published by Information Technology.

Access Control:

- Access to generic accounts should be strictly controlled and granted only to authorized individuals.
- The principle of least privilege should be applied, ensuring individuals have the minimum levels of access required to perform their functions.


Password Management:

- Passwords for generic accounts must be strong and comply with the University's Password Policy.
- Passwords and accounts are not to be shared.
- Passwords for generic accounts are changed annually or when account usages changes or if the account generates security concerns.

Audit and Monitoring:

- Usage of generic accounts must be logged and monitored to ensure compliance with this policy.
- Any misuse or unauthorized access to generic accounts must be reported to the Information Technology department.

Maintenance:

 SOUTHEAST MISSOURI STATE UNIVERSITY · 1873	BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 10/23	Revision Date:	Page: 3 of 3
		Section: INFORMATION TECHNOLOGY		Classification Code: 10-17
		Subject: GENERIC ACCOUNT POLICY		

- Generic accounts must be reviewed periodically, and at least annually, by the requesting department, division, college or organization, to ensure they are still necessary and are being used in accordance with this policy.
- Unused or no longer needed generic accounts must be disabled and deleted in a timely manner.

Documentation:

All activities related to the creation, modification, and deletion of generic accounts must be properly documented.

Training and Awareness:

All users granted access to generic accounts should receive appropriate training and awareness regarding the responsible use of these accounts.

Policy Review and Modification:

This policy should be reviewed at least annually or as deemed necessary by the AD Administration Authority.

Responsibilities:

- Information Technology is responsible for the implementation, enforcement, and periodic review of this policy.
- All University stakeholders are responsible for adhering to this policy.

Enforcement:

- Any violations of this policy are subject to disciplinary action, up to and including termination of employment and/or legal action.

Approval and Revision History:

- This policy must be approved by the Board of Governors. Any revisions to this policy must be documented and communicated to all affected parties.