Salisbury University

Account Management Policy

1. PURPOSE

The Salisbury University Information Technology (SUIT) department is responsible for ensuring the confidentiality, integrity, and availability of Information Technology (IT) systems. Establishing and maintaining a current and accurate account management policy ensures access to the IT infrastructure is provided to only those individuals required to authenticate to the network to perform their assigned duties and roles.

2. REVISION HISTORY

Date	Version	Approved By:	Policy Update
12/18/2017	1.0	Dr. Dudley-Eshbach	Initial Publication
8/29/2018	1.1	Ken Kundell	USM update to require confidentiality agreement

3. SCOPE

This policy applies to IT systems supported by, or under the policy authority of, SUIT. Any IT systems that require, or can be configured with, authentication shall incorporate processes and procedures wherever possible to meet the minimum requirements set within this policy.

4. BASE POLICY AND COMPLIANCE REFERENCES

SUIT policy framework is based upon federal, state, and industry best practices and standards. Below is a listing of the base policy and compliance references from University System of Maryland (USM), Federal, State, and other

organizations. This policy serves as SU's authoritative adaptation of these policies with specific amendments to meet the business and operational needs of the University.

Policy References

- State of Maryland Department of IT - Cybersecurity Policy: http://doit.maryland.gov/Pages/DoIT-Policy-List.aspx
- USM Security Guidelines: http://www.usmd.edu/usm/adminfinance/itcc/USMITSecurityStandards.pdf

5. POLICY

This policy establishes the minimum requirements to effectively manage user, service, system, and network administrator accounts while ensuring access to systems and information are restricted based on assigned roles or specific services.

#	Name	Requirement
A	Account Management Tool	The preferred method of account management at Salisbury University is Active Directory (AD) and it is used to manage all account access wherever possible.
B	Role Based Access	SUIT will use **role-based access control** within any capable system to manage roles and determine level of access needed to perform the duties assigned to those roles. • Identify information and system access based on departmental need and role. • Determine privileged-user roles per administrative function, and design with **least privilege** in mind, e.g., network team personnel need access to switches and routers. • Restrict service account access where feasible to allow ONLY the function required for that service account to perform the necessary functions.
C	Individual Accounts	All users will be issued a unique, individual account; no shared passwords for account will be used unless otherwise authorized through the exemption process and used solely for business purposes after exhausting all other alternatives. Network and system administrators will have a standard user account and another administrative account to use when performing specific functions requiring an elevated privilege.
D	Continuous monitoring	All accounts will be subject to monitoring and data will be logged for compliance and auditing purposes where possible.
E	Account Auditing and Review	Active Directory accounts will be audited periodically to ensure policy compliance and to review access levels and account status. Account creations, deletions, and permission changes will be reviewed for possible network exploitation regularly.

5.1 Approval Process

All SUIT Managed accounts where possible are managed by Active Directory (AD). Approvals for account creation, deletion, and departmental changes are based automatically off contract data from the SUIT HR system. Manual overrides of the automated system must be approved by the appropriate SUIT Director.

5.2 Account Management Procedures

A set of procedures detailing a standardized methodology for creating, deleting, disabling, and maintaining accounts within the University will be established and managed by SUIT.
SUIT ensures that all accounts conform to these procedures and can be audited for information including, but not limited to, the required level of access, account creator, and the list of approvers for any exceptions.
Administrative accounts will be separate accounts for system or network administrators who require specific, elevated privileges to perform the functions of their administrative roles. Blanket or domain administration accounts will be avoided where possible to reduce the scope of damage from any compromised account or insider threat

Service accounts will be created at the discretion of SUIT to allow only the functionality or access required for their specific tasks. These accounts will be maintained as privileged accounts and restricted to administrative personnel who manage the service account, with passwords protected as confidential data.
All accounts must meet the minimum requirements listed below:

- A uniform schema will be used for account identification that will encompass measures to address similar users, e.g., having more than one John Smith.
- Required fields will be identified to facilitate the determination of employee position or role within the agency.
- Upon notice of employee termination, accounts must be disabled by the close of the same business day where possible to prevent the employee from accessing the network or systems and possibly causing harm or data loss.
- PeopleSoft Access will be audited periodically to mitigate permission creep, this ensures no individual account has access to information the user does not need to know or permissions to systems or devices to which the user does not require access.

5.3 Minimum Authentication Requirements

System and network technical controls will be implemented to manage minimum requirements for accounts to authenticate to the network. The following controls will be implemented within the network:

#	Name	Requirement
A	Signed AUP	All users will sign and submit, initially and as the Acceptable Use Policy is updated, an Acceptable Use Form (see *Acceptable Use Policy*) before being granted escalated privileges to administrative systems.
B	Password Length	All Maryland network systems will use passwords at least 14 characters long.
C	Password Complexity	Passwords will be required to have at least three of the following four types of characters contained within it: • Capital letter • Lower case letter • Number • Special characters (such as the shifted number bar; !@#$... etc.).
D	Password History	Technical policies will enforce a 24 password history before an old password can be reused.

E	Maximum Password Age	▪ Employee and Administrator accounts will be forced to change passwords every 90 days ▪ Student accounts will be forced to change passwords every 180 days ▪ Service account passwords may be set to never expire but where possible should be denied local logon or other security measures to protect the accounts.
F	Minimum Password Age	Users will be unable to change a new password without IT assistance (other than an initial password reset) for 1 day.
G	Failed Attempt Lockout	After 6 consecutive failed logon attempts within one minute, the user account will be locked. SUIT personnel will be able to unlock the account prior to lockout expiration
H	Lockout Time Period	Accounts will be locked out for a minimum of 10 minutes before being unlocked automatically.
I	Disabling Accounts	Accounts are controlled by contract data for employees, enrollment data for students or manual affiliations, all of which are maintained in PeopleSoft. As status changes within PeopleSoft, accounts are enabled/disabled/modified to their new role or status.
J	Deleting Accounts	Employee and Student accounts will be disabled for at least six months before being purged from the system, unless otherwise required by specific regulations, standards, or SUIT procedures.

5.4 Auditing

It is the responsibility of SUIT to ensure compliance with this policy. All users will be accountable for their actions and behavior while using the SUIT assets. All users will be required to read and accept the SU Acceptable Use Form (see SU Acceptable Use Policy) when issued an account and take part in regular security training.

Users will be required to protect their accounts and must create secure, unique passwords. SUIT will ensure that the password requirements defined in section 5.3 above are maintained where possible.
A consent-to-monitoring banner will be displayed on SUIT managed systems that are capable of displaying it, and users must accept monitoring before authenticating to the system. User Internet behavior and system interaction will be logged and automatically monitored where possible by SUIT to ensure compliance with policies and to prevent possible exploitation by external or internal threats (see *SU Continuous Monitoring Policy*).

5.5 Cybersecurity Awareness and Training

As part of the onboarding process and the mandatory training requirement, users will:

- Receive training in secure system use
- Be informed of the processes and procedures for handling confidential data, e.g., MD sensitive data, PHI, and PII
- Understand current cybersecurity threats and their potential exposure, e.g., social engineering, malicious code, and inadvertent information exposure.
- Be required to sign a confidentiality agreement.

While much of the training of specific job functions will be handled by the new user's respective department, technical training on properly accessing the systems and information security awareness helps ensure consistent use or best practices and standard operating procedures.

5.6 Segregation of Key Duties

For critical SUIT systems, the functions of system administration, programming, authorizing of business transactions and security role administration should be segregated. In situations where this may not be possible, compensations controls must be established to mitigate the risk.

6. EXEMPTIONS

If an exemption from this policy is required, a SUIT Policy Exemption Form needs to be submitted and it needs to clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks associated with this exemption. If the University can accept the risk, an exemption to this policy may be granted**.**

7. DEFINITIONS

Term	Definition
Least Privilege	The security objective of granting users only those access rights they need to perform their official duties.
Role Based Access Control	A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities.
Service Account	A special user account that an application or service uses to interact with the operating system.
Windows Group Policy	An infrastructure that allows implementation of specific configurations for users and computers, particular to the Microsoft Windows environment.

8. ENFORCEMENT

SUIT is responsible for managing security assessments for the University according to established requirements authorized in the SUIT Security Program Policy. Any systems under the policy authority of SUIT with requirements that deviate from the SUIT Security Program policies are required to submit a Policy Exemption Form to SUIT for consideration and potential approval.

Any attempt by personnel to circumvent or otherwise bypass this policy or any supporting policy will be treated as a security violation and subject to investigation. The results of the investigation may entail written reprimand, suspension, termination, and possibly criminal and/or civil penalties.