Salisbury University

Email Security Policy

1. PURPOSE

Employees and contractors of the State may send or receive **confidential information** via email while conducting business. Confidential information and official correspondence must be exchanged securely and protect agency data. The purpose of this policy is to define acceptable guidelines for sending email containing confidential information. The Salisbury University Information Technology (SUIT) department is responsible for, and committed to, managing the confidentiality, integrity, and availability of SUIT networks, systems, and applications within the scope of its authority.

2. REVISION HISTORY

Date	Version	Approved By:	Policy Update
12/18/2017	1.0	Dr. Dudley-Eshbach	Initial Publication

3. SCOPE

This policy is applicable to all SUIT environments and assets owned or operated by any department supported by, or under the policy authority of, Salisbury University (SU) -- specifically those assigned an email account on a State email system. SUIT will be responsible for ensuring compliance with the policy as outlined in section 5.0 below for all such SU email users.

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 appropriate use of a University-issued email account and applies to all personnel, such as: (1) employees, (2) vendors, and (3) agents operating on behalf of the University.

5.1 General Requirements

#	Name	Requirement
A	Compliance with All Policies	All use of email must be consistent with SUIT policies and processes, including but not limited to the *Acceptable Use Policy*. NOTE: Users will be held accountable and responsible for protecting confidential information and for the proper use of public information
B	Use for Official State Business	All University-issued email accounts should be used primarily for official State purposes; personal communication is permitted on a limited basis as long as it does not interfere with job-related duties and does not lead to the unauthorized distribution of confidential information. Using University-issued email accounts for the purposes of conducting personal business affairs is strictly prohibited (e.g., webhosting, real estate business, or supporting a side business).
C	Confidential Information Security	Data loss prevention (DLP) solutions, where feasible, should filter all email traffic for confidential information.
D	Electronic Communication Ownership	Messages created, sent, and received on a University-issued email are property of the State of Maryland.
E	Monitoring	Messages created, sent, and received through University-issued email may be monitored without prior notice.
F	Attachment Security	Filters will be used to prevent the receipt of unauthorized attachments.
G	Training	Users shall receive training on email security precautions as part of the Security Awareness Training program.

5.2 Automatic Email Forwarding

SU has established controls to ensure that email is retained and stored within the United States where possible, with encrypted backups, and is recoverable for historical analysis.

Employees and contractors for the University may receive confidential information to their Salisbury.edu email addresses and may also conduct official business for the benefit of the University using their Salisbury.edu email addresses. However, no automated exchange of confidential information or official correspondences is permitted; all official email correspondence and all email containing confidential information must be explicitly user-generated and provide the State with the ability to maintain a record of such exchanges.

#	Name	Requirement
A	Automated Forwarding from Salisbury.edu	▪ Automated email forwarding features to an external non-SU mail domain is prohibited from the Salisbury.edu email domain ▪ Exception will only be granted on a case-by-case basis with the written approval of the SU Chief Information Officer with records of exceptions maintained centrally and reviewed annually.
B	Forwarding of Individual Messages	Forwarding of non-confidential email is permitted so long as it is not automated as defined in 5.2.A above.
C	Automated Forwarding to Salisbury.edu	Users are permitted to automatically forward their external mail to a salisbury.edu email address. NOTE: All messages received at the Salisbury.edu email domain become the property of the State of Maryland and as such are subject to monitoring, discovery and all applicable laws and policies of the State of Maryland and SU.

6. EXEMPTIONS

If an exemption from this policy is required, an 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
Confidential Information	Confidential information is non-public information that, if disclosed, could result in a negative impact to the State of Maryland, its employees, or citizens and includes the following sub-categories: ▪ Personally Identifiable Information ▪ Restricted Information For more information on confidential information see SU *Confidential Information Policy.*

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.