Salisbury University

System Development Life Cycle Policy

1. PURPOSE

The purpose of the Systems Development Life Cycle (SDLC) Policy is to describe the requirements for developing and/or implementing new software and systems at the Salisbury University and to ensure that all development work is compliant as it relates to any and all regulatory, statutory, federal, and /or state guidelines.

2. REVISION HISTORY

Date	Version	Approved By:	Policy Update
9/19/2018	1.0	Marvin Pyles	Initial Publication

3. SCOPE

This policy is applicable to all University employees (faculty, staff, and student employees), students, and other covered individuals (e.g., University affiliates, vendors, independent contractors, etc.) that perform any type of software or systems development work under the auspices of the University.

In the event a SU Department or Unit chooses to seek an exemption for reasons such as inability to meet specific points, tasks, or subtasks within the SDLC Policy or Standards, a SDLC Review Committee, comprised of representatives from across campus as designated by Information Technology, will convene in order to assess the specific merits of the exemption request(s) while still adhering to the main principles behind the SDLC Policy and Standards.

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

SU Information Technology (SUIT) at Salisbury University, is responsible for developing, maintaining, and participating in a Systems Development Life Cycle (SDLC) for SU system development projects. All entities at the University, engaged in systems or software development activities, must follow the SU SDLC. This SDLC is detailed in the SU Systems Development Life Cycle (SDLC) Standards document.

SDLC Phases:

- Initiation
- Development / Acquisition
- Implementation / Assessment
- Operations and Maintenance
- Disposal

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. Exceptions to this policy and associated standards shall be allowed only if previously approved by the SU SDLC Review Committee and such approval documented and verified by the Chief Information Officer. If the University can accept the risk, an exemption to this policy may be granted**.**

7. 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.