



**Information Technology Services
Security Control Standards**

NIST Control Family – System and Service Acquisition

| CONTROL NUMBER | CONTROL NAME | PRIORITY | REVISION DATE | NEXT SCHEDULED REVIEW DATE |
|----------------|-------------------------------|----------|---------------|----------------------------|
| SA-3 | System Development Life Cycle | P1 | 4/15/2020 | 4/15/2021 |

I. Statement

All software developed in-house that runs on production information systems shall be developed according to a Software Development Lifecycle (SLDC) plan. At a minimum, this plan shall address the areas of preliminary analysis or feasibility study; security risk identification and mitigation; systems analysis; general design; detail design; development; quality assurance and acceptance testing; implementation; and, post-implementation maintenance and review. The requirement for such methodology ensures the software will be adequately documented and tested before it is used in production.

II. Applicability

This Control applies to all Tarleton network information resources. The intended audience for this Control includes all information resource owners, custodians, and users of information resources.

III. Risk Statement

Developed and implemented systems do not consider the design phase of the systems development lifecycle.

IV. Implementation

The University determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system.