



**Information Technology Services
Security Control Standards**

NIST Control Family – System and Communication Protection

CONTROL NUMBER	CONTROL NAME	PRIORITY	REVISION DATE	NEXT SCHEDULED REVIEW DATE
SC-12	Cryptographic Key Establishment and Management	P1	4/15/2020	4/15/2021

I. Statement

When encryption is used, appropriate key management procedures are crucial. The university is responsible to manage cryptographic keys for required cryptography employed within the university using automated mechanisms with supported procedures.

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

Cryptographic keys are modified, lost, destroyed or disclosed to unauthorized parties.

IV. Implementation

When cryptography is required and employed within the University information system(s), the University establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures. Cryptographic keys managed by the University will be done in a manner to protect keys from disclosure, including proper storage access controls, exchange, and destruction.