Remote Network Access Security Rule

I. Purpose

1.1 Dixie State University IT Services provides remote network access using an enterprise SSL Virtual Private Network (VPN) service. This service is intended to meet the need for access to on-campus IT resources from remote locations for students, faculty, staff, and other campus affiliates.

1.2 Uncontrolled, decentralized remote network access to the DSU network presents significant risks to the security stability of the University network and to sensitive internal University data and personal confidential data stored on University systems. Non-standard remote access systems may bypass safeguards and controls designed to protect the University network and data stored on University IT resources. In addition, remote access services provided by third-parties are not subject to University policies, have no obligation to protect University data, and may not provide audit capabilities to University IT staff and Data Stewards.

II. Rule

2.1 The University VPN provides secure remote access by default to public University IT resources including, but not limited to:

2.1.1 www.dixie.edu and other University Websites

2.1.2 Employee Email

2.1.3 Banner Self-Service System

2.1.4 Learning Management Systems

2.2 Many of the above services are publicly available regardless of University VPN use. However, the University VPN provides a secure network path to access these services and its use is encouraged in circumstances such as Wi-Fi hotspots in airports, hotels, and coffee shops or any other situations where the remote network's security or trustworthiness is unknown or suspect.

2.3 The University VPN is also intended to provide remote access to systems and services that are not publicly available, including terminal or desktop access to office computers. Access to internal IT resources must be arranged through IT Services. Users requesting University VPN remote access directly to the

University Banner INB system, terminal or desktop access to office computers to facilitate access to the Banner INB system, or remote access to other systems containing confidential personal information must receive authorization from their Data Steward or supervisor before IT Services will provision this access.

2.4 Use of the University VPN extends the University network beyond the physical boundaries of the University. Users of the University VPN are responsible for ensuring that any device, whether University or personally owned, used for University VPN remote access complies with University IT security and usage policies and rules.

2.5 Students, faculty, staff, and other affiliates must use the University VPN service provided by IT Services to remotely access internal University IT resources, and may not use non-standard remote access systems or services unless the following conditions are met:

2.5.1 The remote access system or service is the subject of academic instruction, or,

2.5.2 The non-standard remote access system or service is required to perform a function in the course of University business that cannot be met using the University VPN service, or,

2.5.3 The non-standard remote access system or service is required for a vendor or service provider to provide support for a system or product used by the University, and the non-standard remote access system or service provides access only to the affected system or product.

2.5.4 The Data Steward(s) with responsibility over the user, department, and/or IT resource has approved the use of the non-standard remote access system or service.

2.6 Upon discovery of unauthorized non-standard remote access system or service on the University network, University IT staff may, at their discretion, block the non-standard remote access system or service until the involved user(s) has met the above conditions.