Delaware State University

University Area(s) Responsible: Division of Technology and Information Systems; Office of Finance and Administration

Procedure Number & Name: 8-04: Remote Desktop Access Guidelines

Approval Date: 7/11/11

Revisions: _____

Related Policies and Procedures: _____

Introduction

Remote desktop access requires additional security controls to mitigate the increased risks posed by allowing connectivity from outside the DSU office environment. Faculty and staff members also need to be aware of expectation of compensation for working outside of schedule work hours utilizing their personal resources.

Scope

This policy applies to connectivity via terminal services to DSU information resources.

Description

Remote desktop access to DSU provides many benefits. It allows personnel working from home, or some alternate location to connect to DSU information resources.

However, Remote desktop access to DSU can pose a risk of intrusion into the DSU network by unauthorized persons. A virtual private network (VPN) connection must be established during remote access to the desktop. The VPN must provide encryption and secure authentication.

Procedures and Guidelines

Remote desktop access will be granted only after:

1 - A signed request form from the user's supervisor is received.

2 - An email confirmation that these guidelines have been reviewed by the user is received from the supervisor.

(a) All security policies in effect within the DSU office environment must also be observed when remotely accessing DSU resources.

(b) Any personal equipment, including personal home computers, used to connect to

DSU's information resources must meet DSU Remote desktop access requirements, including having an approved antivirus program, firewall, etc. installed and configured with the latest updates. Employees using their personal equipment are responsible for any loss, damage or wear to the personal equipment.

(c) DSU sensitive data is not to be stored on any non-DSU computers, or storage devices.

(d) It is the responsibility of employees to ensure that their DSU owned computers and other equipment are not used by unauthorized persons (including family members) so that only authorized individuals can gain access to any confidential, personal or restricted DSU information.

(e) To prevent unauthorized users from accessing sensitive DSU information, remote users must logoff after completing a remote session. They must also wait until they receive a confirmation of their logoff command from the remotely connected machine before they leave the computer they are using.

(f) DSU is not obligated to assume responsibility for operating costs, home maintenance, renovations, or other costs incurred by employees in the use of their homes or other alternative work locations for Remote desktop access into the DSU network.

(g) The use of Remote desktop access into the DSU network does not entitle* an employee to additional compensation or compensatory time off.

* Additional compensation or time of should be discussed prior to working remotely and is subject to management approval.

Roles and Responsibilities

(a) Information Users are responsible for:

(1) Complying with the procedures and guidelines set forth in this policy.

(2) Protecting their Remote desktop access credentials and devices from disclosure to, or use by, unauthorized persons.

(3) Immediately reporting any suspected unauthorized use of their Remote Desktop Access account or any damage to or loss of DSU computer hardware, software, or data that has been entrusted to their care.

(b) Supervisors are responsible for ensuring that their employees understand and comply with these policies and guidelines.

(c) The Information Systems Officer (ISO) is responsible for auditing the use of Remote desktop access to ensure compliance with the procedures and guidelines set forth in this policy.

(d) The user agrees to abide by all software licensing and security agreements. Access may be revoked at any time for noncompliance with security policies, at the request of a supervisor or because of the negative impact on the overall network performance due to remote access connections.

(e) Remote access privileges will be reviewed upon an employee's change of position or department.