UNIVERSITY OF SOUTH DAKOTA

Policy Number: 5.012
Originating Office: Information Technology Services
Responsible Executive: Vice President for Administration and Technology
Date Issued: 10/01/2011
Date Last Revised: 08/05/2015

Remote Access

Policy Contents

I. REASON FOR THIS POLICY

Members of the USD community require remote access to potentially sensitive information to provide the best possible academic experience to an increasingly mobile student population. Students, faculty, and staff often access potentially sensitive information stored at USD from remote locations such as hotels, airports, restaurants, or their homes. This policy defines the standards for accessing the USD network from remote locations. These standards are necessary to protect the integrity of USD information systems that contain potentially sensitive information such as academic records or research data. This policy will be evaluated on an annual basis to ensure its adequacy and relevancy regarding The University of South Dakota's needs and goals.

Policy last reviewed on 8/5/15 by CIO Management Team

II. STATEMENT OF POLICY

1. USD employees must use approved VPN clients to connect to the USD virtual private network (VPN) prior to accessing USD information technology network resources, such as computers, servers, printers, etc. Access to the VPN must be authenticated, encrypted, and logged.
2. Use of the USD VPN is limited to authorized individuals, including students, faculty and staff, to perform academic, research, administrative, and service functions. Connecting to the USD VPN constitutes acceptance of the USD Network Access Policy as well as consent to monitoring and remote search.
3. Any device that is connected to the USD VPN must be properly secured with operating system patches, antivirus software, etc.

4. Software VPN connections will be automatically disconnected after a period of inactivity. These will also have an absolute limit on connection time, regardless of activity.
5. The USD ITS Help Desk will support the VPN server and client, but VPN connectivity issues related to third party networks are not supported.
6. VPN Server connectivity will be configured and maintained by USD ITS.
7. Remote access to USD information systems that contain sensitive information must require authentication, managed centrally by Information Technology Services (ITS), as well as encryption.
8. Remote access to systems in the cardholder data environment is not permitted.
9. USD employees must use secure protocols, such as Hypertext Transfer Protocol Secure (https), when connecting to web resources containing potentially sensitive information such as email or courseware.
10. Authorized users will be subject to discipline as defined by the South Dakota Board of Regents Acceptable Use of Information Technology Systems for violation of this policy.

III. DEFINITIONS

Cardholder Data: At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code See Sensitive Authentication Data for additional data elements that may be transmitted or processed (but not stored) as part of a payment transaction.

Cardholder Data Environment: The network location which contains systems that process, store, or transmit cardholder data.

Hypertext Transfer Protocol Secure (https): a protocol used by web browsers and servers to exchange information using encryption. Web browsers support https without requiring any additional software.

Primary Account Number (PAN): Acronym for primary account number and referred to as account number. Unique payment card number (typically for credit or debit cards) identifies the issuer and the cardholder account.

Virtual Private Network (VPN): a type of network that transfers information using a secure protocol such as IPsec. This type of network is commonly used by employees who connect to a business network from an insecure network (such as the Internet) to prevent tampering or unauthorized access.

IV. PROCEDURES

Using the VPN: Go to the Install VPN article in Coyote One Stop

for help with installing an approved VPN client on your laptop (or other computing device). A compatible VPN client must be installed and configured before an authorized user connects to the USD network remotely. For security and bandwidth conservation, authorized individuals should disconnect from the VPN when access to the USD network is not required.

Securing your device: Go to the Keeping Your Computer Clean article for help with securing your laptop (or other computing device) with the latest patches and antivirus software. Authorized users must secure their computing device prior to connecting to the USD network, and they are encouraged to install a firewall.

Accessing secure services: The preferred method for accessing web-based resources such as email or D2L is via Coyote One Stop, because it provides links to USD web resources using the appropriate security protocols. More information about securely accessing remote services is available in the VPN Remote Access article in Coyote One Stop.

V. RELATED DOCUMENTS, FORMS AND TOOLS

USD Network Access Policy 5.011

USD Antivirus Policy 5.006

Board of Regents Acceptable Use of Information Systems Policy 7.1