Remote Access to Administrative Systems & Data Policy

Category: UBIT
Responsible Office: Office of the Chief Information Officer
Responsible Executive: Chief Information Officer
Date Established: 1/6/2011
Date Last Revised: 6/24/2013
Date Posted to Library: 9/2/2011

Summary

Remote Access is the process of accessing the university's administrative systems and data from networks that are not controlled by University at Buffalo. This policy defines the appropriate security measures that are required for authorized users to remotely connect to UB administrative systems.

Policy

POLICY STATEMENT

Access to the university's administrative systems and data from networks that are not controlled by the university is restricted to a prescribed multilayer security strategy to defend against malicious attacks, unauthorized access to administrative systems and data, and potential compromise of the remote access device. No other means of remote access to administrative systems will be provided.

Multi-layer Security Strategy

Remote access to UB's administrative systems must comply with the following requirements:

1. An institutionally owned device must be securely configured, including installation and support of the appropriate VPN software, and token key generator software or hardware token (fob).
2. A personally owned device must be securely configured, including installation of the appropriate VPN software and utilize a hardware token (fob).
3. Device configuration, regardless of ownership, must comply with university's recommended procedures for anti-virus, anti-spyware, firewall and vendor security updates.
4. Authorized individuals using two-factor authentication must use the appropriate VPN software exclusively to authenticate sessions to university administrative systems and data.

WARNING: When you use your personally owned device to access UB administrative systems you accept the risk that your device may be required as part of a legal investigation.

BACKGROUND

Access to university administrative systems through non-university networks possess substantial risks to confidential and restricted university data, and to personal information accessible via those administrative systems. The Internet is by design an open and insecure suite of protocols that provide ample opportunity for surreptitious and malicious activities

by interlopers. Applying appropriate workstation configuration procedures and standards, and implementing multi-layer security controls will better protect university administrative systems from hackers. Accordingly, two-factor authentication for authorized users is necessary is to ensure data stream encryption for sessions through the Internet.

APPLICABILITY

This policy is immediately applicable to the following administrative system and data:

Administrative System	Effective Date
HUB (UB's PeopleSoft student information system implementation)	1/7/2011

DEFINITIONS

VPN - Virtual private network is an encrypted communications channel between the device and the University network. VPN access is specific to the role of the individual (AdminVPN for HUB administrative users; CITVPN for system support staff).

Device - institutionally or privately owned computing device (laptop, desktop, tablet, smartphone) capable of supporting the appropriate VPN software, token key generation software or utilize a hardware token (fob) to establish a work session to university administrative applications through the Internet.

Securely configured – adhering to the guidelines and practices within UB's policy for Securing Network Connected Devices

Hardware Token – a physical device that is assigned to an authorized individual that is used to prove the individual's identity electronically

RESPONSIBILITY

The Information Technology Policy Officer is responsible for the maintenance of this policy, and for responding to questions regarding this policy. The Chief Information Officer is the responsible officer.

PROCEDURES

Implementing this policy provides you with required, multi-layered protection from malicious programs and unauthorized access. Failure to implement these security controls may result in the workstation being compromised, university data placed at risk, as well as risks to personal protected information. If your machine is compromised and it is remotely connected to the university's network, the university will immediately prohibit your connection until corrective actions are taken.

Contact Information

For more information about this policy, contact the

Office of the CIO
517 Capen Hall
University at Buffalo
716-645-7979

Related Information

University Documents:

- *UB Computer & Network Use Policy*
- *Information Security: Data Access and Security Policy*
- *Protection of Regulated Private Data Policy*
- ***Securing Network Connected Devices***