

Remote Access Policy

Policy

Remote access to information technology resources (switches, printers, routers, computers, etc.) and to sensitive or confidential information (social security numbers, credit card numbers, bank account numbers, etc.) are only permitted only through secure, authenticated and centrally-managed access methods. Authorized users of Darton College's computer systems, networks or data repositories are only permitted to remotely access these systems, networks or data repositories for the conduct of university-related business.

Rationale

Increases in non-traditional teaching methods and the increased mobility of faculty and students have made remote access to centralized university assets increasingly important. Opening uncontrolled or unsecured paths into any element of the university network or internal computer systems presents additional risk to the entire university infrastructure. Establishing policy centrally and issuing standards from a central authority allows a minimum number of penetrations of the security of the network while still allowing flexibility in the actual remote connection technology used.

Standards

A virtual private network (VPN) connection must be established during the off-site remote access of university information technology resources (switches, printers, routers, computers, etc.).

The Information Security Department will be contacted when the use of a VPN is not viable, when additional controls are required, or for "pass list" requests.

Remote Access to Sensitive Information. Systems that contain sensitive student, personnel and financial data will be available for off-site remote access through a centrally managed VPN that provides encryption and secure authentication. Access may be revoked at any time for reasons including non-compliance with security policies, request by the user's supervisor or negative impact on overall network performance attributable to remote connections. Remote access privileges for university information will be reviewed upon an employee's change of departments.

Access/Authentication. The access and authentication system for remote access will be centrally managed.

Endpoint Security. External computers that are used to administer university resources or access sensitive information must be secured. This includes patching (operating systems and applications), possessing updated anti-virus software, operating a firewall and being configured in accordance with all relevant university policies/procedures.