

Columbus State University ZENworks Remote Control Policy

Created July 18, 2007

1.0 Background

The CSU network consists of over 2,500 computers located in nearly all buildings on two campuses, as well as in outlying facilities. CINS is responsible for maintaining all campus computers and supporting their use by approximately 800 faculty and staff users and over 7,000 students. ZENworks Remote Control is a product that allows CINS technicians to resolve service requests by remotely controlling a user's computer. As a result, CINS can make the most of limited resources while servicing customers more efficiently.

2.0 Purpose

This policy sets forth guidelines for the use of ZENworks Remote Control to facilitate desktop support services.

3.0 Policy

- All CSU computers must include the ZENworks client as part of normal operations.
- Only CINS staff (not student assistants) may initiate a ZENworks Remote Control session.
- CINS may only initiate a session when the user requests assistance and is agreeable to a solution involving Remote Control.
- By default, the user will have the choice to accept or reject Remote Control sessions.
- CINS cannot override a rejection or force a computer to accept a Remote Control session.
- Remote Control sessions will not allow file transfers *from* the user's computer to the technician's computer. CINS may only transfer files *to* the user's computer.

4.0 Procedures and Responsibilities

- Based on the nature of the request, the technician will determine whether the request can be resolved using Remote Control.
- The technician will contact the user via telephone prior to initiating a Remote Control session.
- Users should close all applications other than those needed in order to resolve the issue.
- Users should remain at their computer during the session.
- CINS is responsible for the appropriate use of ZENworks Remote Control and must respect the user's privacy at all times.