REMOTE VIEWING AND CONTROLLING OF WORKSTATIONS
GUIDELINES FOR AUTHORIZING REMOTE VIEW OR CONTROL

Issued March 1, 2007 from IT Networks and Security. These guidelines are based upon materials prepared by the HIPAA Compliance Office and Business Services Computing. Questions about these guidelines can be addressed to itap-securityhelp@purdue.edu.

I. Introduction:

Many support areas across campus use tools that allow them to remotely view or remotely control a customer’s workstations to assist with troubleshooting computer hardware or software issues.

These capabilities add risks to security and privacy as the support personnel can view what is on a screen in real-time and assist in troubleshooting technical issues or difficulty. When granted remote control access, support personnel also have access to any application or function to which a user has been given rights.

II. Guidelines for Authorizing Remote View or Control of Workstations

Users should follow these guidelines when authorizing remote view or control of a workstation:

- Do not accept remote view or remote control requests that you did not initiate. (Example: If you have not reported that you are having a problem to your technical support staff, you should not accept remote view or control requests if you are contacted by an individual to fix an issue.)

- Always remain alert against possible “social engineering” attempts via phone or email and report any unsolicited requests for remote view or control of your workstation to your supervisor. Do not accept remote view or remote control requests that you did not initiate.

- Only allow remote view or remote control access to your workstation when absolutely necessary and only grant permission to remote view or remote control to your area’s appropriate support personnel. If you are not sure whether support personnel should be granted remote view or remote control access to your workstation to resolve a problem, do not grant permission to remote view or remote control and request guidance from your supervisor.

- Close all applications that are not needed in order to resolve the issue for which you are obtaining support.

- Remain at the workstation during the time your workstation is remotely viewed or controlled. Do not leave your workstation unattended while it is remotely viewed or controlled.
REMOTE VIEWING AND CONTROLLING OF WORKSTATIONS
GUIDELINES FOR AUTHORIZING REMOTE VIEW OR CONTROL

Issued March 1, 2007 from IT Networks and Security. These guidelines are based upon materials prepared by the HIPAA Compliance Office and Business Services Computing. Questions about these guidelines can be addressed to itap-securityhelp@purdue.edu.

- Watch carefully the actions taken by others who are remotely controlling your workstation. Per policy, you are responsible for any actions taken while you are logged into your system account. If you are uncomfortable with actions taken during a remote view or remote control session, immediately end the session and notify your supervisor.

- Never provide your password or any other authentication credentials (such as a PIN, token, passphrase) to remote view or remote control support personnel. Never allow remote view or remote control support personnel to view an unobscured/unmasked password.

- Ensure that any remote view or remote control session is disconnected and/or terminated after the support personnel have completed assisting you.

- If you are uncomfortable with actions taken during a remote view or remote control session, immediately end the session and notify your supervisor who will report the incident according to Purdue’s Incident Response Policy (VII.B.3).

III. Related References


Revised November 21, 2011 to update URLs.