MEMORANDUM

To: USC Faculty and Staff

From: Laura LaCorte, Associate Senior Vice President for Compliance
Ilee Rhimes, CIO and Vice Provost for Information Technology Services

Date: January 7, 2013

Subject: Important Changes for Users Remotely Accessing USC Systems

If you use remote access programs to connect to your USC desktop or other USC systems, please read this memorandum carefully. Beginning in January 2013, USC account holders will need to use USC's Virtual Private Network (VPN) to access USC systems remotely. (Please be advised that access to library resources through the USC Libraries website will not be affected by this change.)

Information security breaches have become an unfortunately common occurrence across the world. Cyber attackers, or hackers, are sophisticated, organized, and persistent in their efforts to successfully identify and exploit vulnerabilities in information technology (IT) systems. Without proper safeguards, USC faculty, staff, and students can become victims of these attacks, which could result in loss of passwords, data, and privacy, and could even lead to identity theft. One of these safeguards is the use of USC's VPN (IP tunneling) to connect securely to the USC network prior to accessing USC systems remotely.

When used without a VPN, remote-access applications, such as Windows Remote Desktop Protocol (RDP), represent one of the most common attack vectors exploited by hackers, creating vulnerabilities for the USC network, USC information systems, and the faculty and staff using the applications.

As of **January 28, 2013**, the university will restrict direct access to the USC network using RDP. USC faculty, staff, student workers, and third parties with access to USC systems will be required to use USC's VPN before they remotely access their USC servers, laptops, desktops, or workstations. VPN encrypts traffic to prevent others from viewing the information while it is in transit and is a more secure method of accessing USC computer resources. Health IT supported users may continue to use the secure Citrix solution provided via the Keck Portal as an alternative.

University of Southern California
3500 South Figueroa Street, #105, Los Angeles, California 90089-8007 • Tel: 213 740 8258 • Fax: 213 740 9657 • complian@usc.edu

You can install VPN software by following instructions at www.usc.edu/its/vpn. For step-by-step video tutorials, created by the IT team at the USC Price School of Public Policy, and written instructions that cover installing VPN on devices running specific operating systems, see the following links:

Windows XP, Windows Vista, and Windows 7 devices:
www.usc.edu/its/vpn/anyconnect.html

Mac 10.4 (Tiger) and later devices:
www.usc.edu/its/vpn/anyconnectmac.html

iOS (iPhone and iPad) devices:
www.usc.edu/its/vpn/anyconnectios.html

Between now and the January 28 deadline, our offices will be working with the school/unit IT administrators to assist users with installing VPN. If you need assistance, contact the ITS Customer Support Center at 213-740-5555 or your IT administrator. A list of school/unit IT contacts is at: www.usc.edu/its/contact/school_list.html.

To review the university's Network Infrastructure Use Policy, please refer to http://policies.usc.edu/p5infoTech/network_use.pdf. For information about USC's information security education program, go to www.usc.edu/compliance. As a security reminder, see cio.usc.edu/password for tips on selecting strong passwords.

For questions about this memorandum, please contact Information Security, in the Office of Compliance, at (213) 821-2614 or infosec@usc.edu.

cc: Todd Dickey
Elizabeth Garrett