UNC School of Dentistry Personally-Owned Computing Device Policy (BYOD)

Introduction

Purpose of Policy

To establish how SoD faculty, staff and students will use and access the dental school's information systems, servers and services using personally-owned computing devices.

Audience

All UNC SoD faculty, staff, students, visitors, temporary employees and vendors who desire access to the dental school's information systems, servers and services with personally-owned computing devices.

Definitions

BYOD(s) – Bring your Own Device(s) – A personally-owned computing device that will be used to access the dental school's information systems, servers and services and that processes and/or stores digital information, including but not limited to computers, smartphones and tablet computers. This includes any CCI laptop that does not or cannot conform for technical or OCIS computer support reasons with the University's Information Security policy on securing mobile devices.

CCI – Carolina Computing Initiative. The UNC campus computing program developed in 1997 to ensure that Carolina students, faculty and staff have easy access to high-quality and affordable technology.

Dongle - A small piece of hardware that plugs into an electrical connector on a computer and serves as an electronic "key" for a piece of software; the program will run only when the dongle is plugged in.

NAC – Network Access Control. NAC is a proactive, end-user networking solution for wired and Wi-Fi connections that identifies potential security problems on a computer before it accesses the UNC or SoD network.

OCIS –The SoD's IT Department. The Office of Computing and Information Systems.

P2P - Peer-to-peer file sharing (P2P) allows users to download media files such as music, movies, and games using a P2P software client that searches for other connected computers. The "peers" are computer systems connected to each other through the Internet.

Smartphone - A smartphone is a mobile phone built on a mobile operating system, with more advanced computing capability and connectivity than a feature phone

SoD – UNC School of Dentistry.

SoD email – The SoD's electronic mail system. SoD's email is considered by the school as sensitive because of the transmission and receipt of HIPAA-related information between faculty, staff, students and external health care providers.

Tablet – A slate computing device which is a class of mobile computer (e.g. iPad, Android pad, Kindle, Blackberry Playbook, Windows Slate PC, etc.) that accepts input from an electronic pen or finger input rather than from a keyboard.

UNC-ISO – The University Information Security Office. The University's Information Security Office oversees the security of the University's electronic information.

Policy

Policy Statement

The SoD will allow the use of BYODs to access dental school information systems, servers and services if it can through OCIS maintain the security of confidential University data and/or SoD sensitive information the device could access.

The acceptance and support of BYODs for a person or a program should not affect OCIS' ability to provide prompt technical support to SoD non-BYOD and University-owned faculty, staff and student computers and devices. Technical support for the SoD's non-BYOD users and its University-owned devices will always take priority over any OCIS technical support provided to BYOD users and devices. This does not include the support of OCIS approved SoD applications delivered in a terminal server, cloud computing, virtual PC or web application environment and it does not include SoD applications that have been approved by the OCIS Director or his delegate to be installed and supported by OCIS on a BYOD computer.

BYODs must be reviewed by OCIS and approved by the OCIS Director or his delegate before access to dental school information systems, servers and services is granted. The OCIS Director or his delegate reserves the right to rescind BYOD access to SoD systems, servers or services for a person or a program if at any time University data is suspected to be at risk because of BYOD or continuing support of the BYOD device or program frequently affects providing prompt support of SoD's non-BYOD and University-owned faculty, staff and students' computers and devices.

BYOD users are required to adhere to and comply with all University Information Security policies and standards for acceptable use and accessing University systems, servers and services. This policy does not supersede any existing University policy or applicable state or Federal laws.

Compliance

Compliance Statement

Failure to adhere to the security sections of this policy, its procedures or standards may put University information at risk and may have disciplinary consequences for employees up to and including the termination of employment. Students who fail to adhere to the security sections of this policy, its procedures or standards will be referred to SoD Office of Academic Affairs. Contractors and vendors who fail to adhere to the security sections of this policy, its procedures and standards may face termination of their business relationships with the SoD.

Failure to adhere to the non-security related sections of this policy, its procedures and standards may affect the ability of OCIS to provide prompt, technical support to the school's faculty, staff and students. People and programs that fail to adhere to the non-security related sections of this policy, its procedures and standards may have their BYOD privileges suspended or revoked or lose access to SoD systems, servers or services from the BYOD device.

Procedures

All

Any person with a valid SoD user account is permitted access from any computing device that does not directly store or process sensitive information as defined by the University to access OCIS approved SoD systems, servers and services that are delivered in a terminal server, cloud computing, virtual PC or approved web application environment (e.g. web-mail and remote access to EPR through terminal services that require no physical device connection requirement including external devices like signature pads, sensors, probes, cameras, dongles, special printers, program-specific applications, program-specific systems, program-specific servers and/or services).These devices are not required to be registered in the SoD computer inventory.

Faculty and Staff

SoD faculty and staff members who wish to use a BYOD must submit the device to OCIS for its review for acceptance to use on the SoD network and to access SoD systems, servers and services. The OCIS staff will review the device, determine if and how the device can safely access SoD system, servers or services and make recommendations if needed to ensure the device meets University policy in accessing University and SoD resources. The OCIS Director or his delegate will approve or deny acceptance of the device. If rejected, the OCIS Director or his delegate will state the reasons for rejection.

SoD faculty and staff who wish to use a BYOD smartphone or tablet to directly access the SoD's email and/or calendar system must submit the device to OCIS for its review or optionally follow an OCIS-prescribed self-provisioning and security process for acceptance to use their BYOD

smartphone or tablet on the SoD network and to directly access SoD systems, servers and services. The OCIS staff will review the device, determine if and how the device can safely access SoD system, servers or services and make recommendations if needed to ensure the device meets University policy in accessing University and SoD resources. The OCIS Director or his delegate will approve or deny acceptance of the device. If rejected, the OCIS Director or his delegate will state the reasons for rejection.

Students

SoD programs and departments must request permission to BYOD on behalf of its entire class of students (DDS, DA, DH, Residents, etc.) to use the student's personally-owned laptop computer to access the SoD network and to access SoD systems, servers and services.

SoD programs or departments are responsible for clearly communicating as part of the BYOD request any device or software required by the program or department that needs to connect to or execute on a BYOD (e.g. external devices [signature pads, sensors, probes, cameras, dongles, special printers, etc.], program-specific applications, program-specific systems, program-specific servers and/or services) when requesting BYOD for their class of students to determine if a BYOD device is compatible with those requirements.

A faculty program representative will broadly define the type of device(s) requested by the class to BYOD (e.g. Windows computers, Apple computers or Linux computers) as a part of its BYOD request.

The OCIS staff will review the request, asking the requestor for additional or clarifying information if necessary, determine if and how the device can safely access SoD systems, servers or services and make recommendations if needed to ensure the device meets University policy in accessing University and SoD resources.

The OCIS Director or his delegate will approve or deny acceptance of the classes' devices to the program's or department's requestor. If rejected, the OCIS Director or his delegate will state the reasons for rejection.

SoD students who wish to use a BYOD smartphone or tablet to directly access the SoD's email and/or calendar system must submit the device to OCIS for its review or optionally follow an OCIS-prescribed self-provisioning and security process for acceptance to use their BYOD smartphone or tablet on the SoD network and to directly access SoD systems, servers and services. The OCIS staff will review the device, determine if and how the device can safely access SoD system, servers or services and make recommendations if needed to ensure the device meets University policy in accessing University and SoD resources. The OCIS Director

or his delegate will approve or deny acceptance of the device. If rejected, the OCIS Director or his delegate will state the reasons for rejection.

Others

Any other person associated with the SOD but is not a student, faculty or staff must be sponsored by a SoD faculty or staff who will justify to the OCIS Director or his delegate why the person needs access to SoD systems, servers or services. The person will then submit the device to OCIS for its review for acceptance to use on the SoD network and to access SoD systems, servers or services. The OCIS staff will review the device, determine if and how the device can safely access SoD system, servers or services and make recommendations if needed to ensure the device meets University policy in accessing University and SoD resources. The OCIS Director or his delegate will approve or deny acceptance of the device. If rejected, the OCIS Director or his delegate will state the reasons for rejection.

Any other person associated with the SOD but is not a student, faculty or staff and who is sponsored by a SoD faculty or staff and who wishes to use a BYOD smartphone or tablet to directly access the SoD's email and/or calendar system must submit the device to OCIS for its review or optionally follow an OCIS-prescribed self-provisioning and security process for acceptance to use their BYOD smartphone or tablet on the SoD network and to directly access SoD systems, servers and services. The OCIS staff will review the device, determine if and how the device can safely access SoD system, servers or services and make recommendations if needed to ensure the device meets University policy in accessing University and SoD resources. The OCIS Director or his delegate will approve or deny acceptance of the device. If rejected, the OCIS Director or his delegate will state the reasons for rejection.

Standards

General

A BYOD laptop must meet minimum University technical specifications to access the University's network. The current specifications can be found at http://cci.unc.edu/new-students/minimum-laptop-requirement/

BYOD devices are required to be registered in the SoD Computer Inventory.

Any exceptions to the BYOD Policy standards (except the sensitive information standard which must also be approved by the UNC ISO and the Dean of the SoD) must be approved in writing by the Director of OCIS.

Security

Computers

A BYOD laptop cannot store or process any confidential or sensitive information as defined by the University.

Exceptions to this standard must be approved in writing by the UNC-ISO, the OCIS Director and the Dean of the SoD.

In the event that a BYOD is authorized to store or process sensitive information, it will be required to comply with the University Information Security Standards for Laptops, Smartphones and PDAs that Store or Process Sensitive Information.

BYOD computers are prohibited from running P2P file sharing applications on the SoD network. The existence of these programs on a BYOD computer places the user in violation of this policy.

BYOD computer users are responsible for ensuring their computer meets minimum campus computer security requirements for antivirus software, ongoing software security patching and device firewall installation and configuration.

BYOD laptops are prohibited from using any email client that stores or caches email onto the laptop's hard drive.

BYOD computers are required to install the University's NAC agent to ensure compliance with required security software.

OCIS and the UNC-ISO reserve the right to prevent the BYOD from accessing University or SoD systems, servers or services if the NAC agent detects a violation of University Security Policy standards.

OCIS may require the installation of software on a BYOD computer to monitor the presence of confidential University data or SoD sensitive information.

Smartphone and Tablets

BYOD smartphones and tablets that directly access SoD email are required to enable the device's onboard device encryption, failed password attempt lockout, required password and remote device wipe capabilities.

OCIS and the UNC-ISO reserve the right to monitor a BYOD smartphone or tablet's access to SoD email and perform a remote wipe of the device and/or installed storage cards if University data or sensitive information may be at risk.

BYOD smartphones or tablets are prohibited from saving confidential University or sensitive data on unencrypted storage cards installed in a BYOD smartphone or tablet computer.

BYOD smartphone or tablet users are responsible for ensuring their device meets minimum campus computer security requirements for recommended antivirus software and required ongoing software security.

BYOD smartphones or tablets are prohibited from running P2P file sharing applications on the SoD network. The existence of these programs on a BYOD smartphone or tablet places the user in violation of this policy.

SoD Email

BYOD smartphones and tablets that directly access SoD email are required to use Microsoft ActiveSync or Blackberry Enterprise Server (BES) to connect to the email server.

Software

BYOD laptop users may be required by OCIS to have the fully supported UNC version of Windows installed on the BYOD laptop either natively or in a dual boot configuration to ensure successful access SoD systems, servers or services.

BYOD computer, smartphone and tablet users are responsible for ensuring their BYOD has the proper version of local applications installed to access SOD systems, servers or services.

Related Data

Appendices

Statutes

US Health Insurance Portability and Accountability Act of 1996. Public Law 104-191
NC Identity Theft Protection Act of 2005. Session Law 2005-414 and Senate Bill 1048.

Policies

Data Network Acceptable Use Policy
Password Policy for General Users
Policy on Peer to Peer File Sharing Programs and PHI
Transmission of Protected Health Information and Personal Identifying Information Policy Contacts
UNC Information Security Policy

Contacts

Questions

David B. Rankin, IT Director SoD, 919-537-3485

Violations

David B. Rankin, IT Director SoD, 919-537-3485

Consulting

OCIS Staff, 919-537-3485
UNC Help Desk, 919-962-4357
UNC Information Security Office, 919-445-9393

History

Effective Date - February 1, 2013
Revised Date – March 4, 2013, Version 0.1
Next Review Date -February 1, 2014

Authorization

Jane A. Weintraub, Dean, UNC School of Dentistry

Signature _____

Date _____