Computer Security Updating Policy

Policy/Procedure

Introduction

The ever-increasing threat to campus operations and institutional reputation in the event of data theft, data loss, or system downtime, due to malicious intrusion, underscores that the security of College-owned technology must be the highest priority.

The technical controls used by IS provide an essential foundation for this security. However, technology only constitutes a portion of the solution; the most effective defense against malicious threats are user awareness of, and diligence in upholding, secure computing practices.

This policy outlines Dickinson's approach to the deployment of security patches and application updates to all College-owned employee and classroom computers. Awareness and compliance with this policy will ensure that consistent computer security levels are maintained campus-wide in an attempt to keep data and users safe, and minimize exposure to security breach.

Library and Information Services reserves the right to apply security measures and updates, and modify operating system settings and functions on College-owned computers in the interests of protecting College data and the College community as a whole.

Update Overview

Security patches and application updates for College-owned Windows and Macintosh computers used by faculty, administrators, or staff will be applied every Thursday evening at 8PM. Critical security and operating system updates will be applied on the Third Thursday of every month at 6PM. All updates for classroom, lab, or shared location Windows and Macintosh computers will be applied nightly at 3AM. Please see below for methodology and schedule details.

Deployment Methodology

User Services distributes security patches and application updates to College-owned Windows and Macintosh computers on different schedules based on the primary use of the computer and the nature of the updates.

Employee Computer Deployment Schedules

For computers used by faculty, administrators, or staff, updates are deployed to computers as follows:

Weekly Updates	
Payload:	Security patches and updates to standard applications installed on the computer.
Schedule:	Every Thursday starting at 8PM.

Power State:	Computer must be turned on in order to receive updates. (** see sustainability section below*)
Login State:	Computer will attempt to install updates regardless of whether anyone is logged onto the computer or not. PLEASE SAVE YOUR WORK AS THE COMPUTER WILL REBOOT REGARDLESS OF ANY OPEN APPLICATIONS AND/OR UNSAVED WORK.
Failover:	If the computer is not powered on during the scheduled update, application updates will be applied the next time the computer is turned on.
IF a User IS Logged In	
Overview:	The computer will attempt to install updates, prompting the user with flexible installation and reboot options to accommodate user work schedule. Updates will be applied and the computer will be rebooted given a lack of response to prompts.
Notifications:	The user may see a small blue Dell KACE window on right side of the screen at any/all of these instances: • Prompting the user to install pending updates or snooze the install • When updates are being installed • Prompting the user that a reboot is required or snooze the reboot
"Snoozing":	The user may postpone ("snooze") installing updates up to five (5) times before the computer will proceed with the installation. Snoozing lasts 1 hour before the user is re-prompted.
Snoozing Timeout:	If the update is not snoozed within 30 minutes, updates will automatically begin installing.
Reboot Snoozing:	If an update is applied which requires a reboot, the user may snooze the reboot up to seven (7) times before the computer will automatically reboot in order to complete the installation. Snoozing lasts 30 minutes before the user is re-prompted.
Reboot Timeout:	If the reboot is not snoozed within 30 minutes, the computer will re-prompt in 120 minutes (ie. another snooze). After the seven (7) snoozes noted above, the user will be forced to reboot the computer.
Reboot Frequency:	If an update is applied which requires a reboot, the computer will reboot once. Any additional reboots required after that will be applied the following Thursday.
Performance Impact:	Application updates vary in number and size at any given time. Impact to computer performance is generally negligible with a possible reboot after installation.

IF NO User Is Logged In	
Overview:	The computer will install updates and automatically reboot if necessary.
Notifications:	None.
Reboot Frequency:	If an update is applied which requires a reboot, the computer will reboot once. Any additional reboots required after that will be applied the following Thursday.

Employee Computer Deployment Schedules (cont.)

Critical "Third Thursday" Monthly Updates	
Payload:	Critical operating system security patches.
Schedule:	The Third Thursday of Each Month starting at 6PM.
Power State:	Computer must be turned on in order to receive updates. (* *see sustainability section below*)
Login State:	Computer will attempt to install updates regardless of whether anyone is logged onto the computer or not. PLEASE SAVE YOUR WORK AS THE COMPUTER WILL REBOOT REGARDLESS OF ANY OPEN APPLICATIONS AND/OR UNSAVED WORK.
Failover:	If the computer is not powered on during the scheduled update, critical updates will be applied when the computer next checks in with the update server.
IF a User IS Logged In	
Overview:	The computer will attempt to install updates, prompting the user with installation and reboot options to assure installation. Updates will be applied and the computer will be rebooted given a lack of response to prompts.
Notifications:	The user may see a small blue Dell KACE window on right side of the screen at any/all of these instances: • Prompting the user to install pending updates or snooze the install • When updates are being installed • Prompting the user that a reboot is required or to snooze the reboot
"Snoozing":	The user may postpone ("snooze") installing updates up to two (2) times before the computer will proceed with the installation. Snoozing lasts 30 minutes before the user is re-prompted.

Snoozing Timeout:	If the update is not snoozed within 30 minutes, updates will automatically begin installing.
Reboot Snoozing:	If an update is applied which requires a reboot, the user may snooze the reboot up to three (3) times before the computer will automatically reboot in order to complete the installation. Snoozing lasts 30 minutes before the user is re-prompted.
Reboot Timeout:	If the reboot is not snoozed within 30 minutes, the computer will automatically reboot and a visual 10-minute countdown until reboot will be provided on the screen.
Reboot Frequency:	If an update is applied which requires a reboot, **the computer will reboot as many times as necessary to complete the critical update installation**.
Performance Impact:	While critical updates vary in number and size at any given time, they are generally larger than weekly updates. Impact to computer performance may vary from negligible to mild sluggishness depending upon which updates are installed with multiple possible reboots after installation.
IF NO User Is Logged In	
Overview:	The computer will install updates and automatically reboot as many times as necessary.
Notifications:	None.
Reboot Frequency:	If an update is applied which requires a reboot, **the computer will reboot as many times as necessary to complete the critical update installation**.

Classroom Deployment Schedules

For computers used in a classroom, lab, or shared location, update are deployed to computers as follows:

Daily Updates	
Payload:	Critical operating system and application security patches.
Schedule:	Every day at 3AM.
Power State:	Classroom Windows and Mac computers will power themselves on at 3AM in order to receive updates.
Login State:	Computer will attempt to install updates regardless of whether anyone is logged onto the computer or not. PLEASE SAVE YOUR WORK

	AS THE COMPUTER WILL REBOOT REGARDLESS OF ANY OPEN APPLICATIONS AND/OR UNSAVED WORK.
Failover:	If the computer is not powered on during the scheduled update time, updates will be applied the next day at 3AM.
IF a User IS Logged In	
Overview:	The computer will attempt to install updates, prompting the user with less flexible installation and reboot options to assure installation. Updates will be applied and the computer will be rebooted given a lack of response to prompts.
Notifications:	The user may see a small blue Dell KACE window on right side of the screen at any/all of these instances: • Prompting the user to install pending updates or snooze the install • When updates are being installed • Prompting the user that a reboot is required or snooze the reboot
"Snoozing":	The user may postpone ("snooze") installing updates up to five (5) times before the computer will proceed with the installation. Snoozing lasts 15 minutes before the user is re-prompted.
Snoozing Timeout:	If the update is not snoozed within 15 minutes, updates will automatically begin installing.
Reboot Snoozing:	If an update is applied which requires a reboot, the user may snooze the reboot up to five (5) times before the computer will automatically reboot in order to complete the installation. Snoozing lasts 20 minutes before the user is re-prompted.
Reboot Timeout:	If the reboot is not snoozed within 15 minutes, the computer will automatically reboot.
Reboot Frequency:	If an update is applied which requires a reboot, **the computer will reboot as many times as necessary to complete the critical update installation**.
Performance Impact:	Critical updates vary in number and size at any given time. Impact to computer performance may vary from negligible to mild sluggishness while updates are installed.
IF NO User Is Logged In	
Overview:	The computer will install updates and automatically reboot as many times as necessary.
Notifications:	None.

	Reboot Frequency:	If an update is applied which requires a reboot, **the computer will reboot as many times as necessary to complete the critical update installation**.

Self-managed Computer Updates

Users are encouraged to manually apply critical patches and application updates on their own when it best suits their schedule. Applying these updates in a timely manner will mean the Dell KACE update server will have less, or nothing, to do when it periodically checks the computer.

Update Testing and Reversal

Occasionally, an update is released which may adversely affect one or many computers due to conflicting resources and/or unintentional manufacturer coding errors. Prior to updates being deployed to campus, User Services tests patches and updates on a selection of monitored computers (which includes the primary computers used by IS staff) to assess and assure update validity, quality, and performance.

In the event an update is deployed to campus which is found to adversely affect computers, User Services will attempt to halt further distribution of the update and, depending on dispersion and variables related to how the update is installed, may attempt to reverse the update back out of computers where it has been installed. The reversal process may result in additional notifications to logged on users and may also require additional reboots to compete the uninstallation process.

Ransomware, Data Loss, and Remediation

While IS makes every effort to keep College-owned computers secure from malicious attack, there is no guarantee that a computer is completely safe from data theft, data loss, or system downtime. As such, it is the user's responsibility to assure that either their data is backed up, or being backed up regularly, and assure that their computers are available to receive updates during the update schedules outlined above. User Services can assist users in backing up their data to Office 365 OneDrive or another equally secure backup location.

If a College-owned computer is compromised and rendered inoperable due to malicious intrusion, User Services will assist in remediating the computer or reimaging it to eliminate the threat. If data is lost due to theft and/or deletion, in-place encryption as a result of ransomware infection, or any other destructive vector, User Services will assist in attempting to recover or restore that data if possible. User Services will not apply funding to recover lost or inaccessible data (ie. paying a third party company for assistance, paying ransomware ransoms, etc.). Lastly, adherent to the Personal Computing Support Policy, User Services staff will neither repair nor remediate personally owned computers.

Sustainability

While User Services is greatly committed to Dickinson's sustainability initiatives and strives to reduce campus computing power consumption where possible, the threat to campus operations and institutional reputation due to data theft, data loss, or system downtime must take highest priority. Therefore, it is critical that computers remain turned on during the update timeframe to assure system integrity and campus security. While IS may apply settings to automatically turn on employee desktop computers so that they may receive scheduled critical updates, once updates have been installed, computers will enter hibernation mode after 90 minutes in order to reduce power consumption.

Related Information

History/Revision Information

Responsible Division/Office: LIS/User Services

Effective Date: 6/19/2017

Last Amended Date: 3/24/2021

Next Review Date: 3/24/2023

Also Found In: