SECURITY MATTERS: University protection of **your data**

The University of Chicago strives to protect the data of its faculty, students, and staff. This data ranges from original research, protected student data, confidential personnel files, private correspondence and federally protected data. When your data and the university's data is lost, stolen, or compromised, the basic privacy needed to conduct your personal life, research, or work is threatened.

A key part of this effort is to make sure laptops, desktops and other common devices are protected on a day-to-day basis in the event they become lost, stolen or compromised. With faculty input, the university has developed a handful of basic best practices.

To help with understanding these basic best practices, we've described what each one means, and how following it protects you. If your devices are managed by your division or unit, they should follow these basic best practices. If it is your own personal device, ask for help.

Get your device(s) encrypted:

Without encryption, the data on a lost or stolen device is no longer under your control. Depending on the sensitivity of that data, the university may have a legal reason to investigate further. With encryption, the data on the stolen or compromised device is useless and inaccessible.

Enable your device(s) to automatically receive security and application updates:

Updates to your computer's operating system and applications often include critical patches to security holes which can be exploited. Enabling this feature ensures your device(s) is up-to-date without needing your manual intervention. In addition to security fixes, updates can also include new or enhanced features, or better compatibility with different devices. Keep in mind that many hackers look for outdated software with unpatched security flaws.

Have antivirus software installed that automatically checks for daily updates:

Antivirus software prevents, detects, and removes software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system (aka 'malware'). This malicious software can not only harm your device but can also spread harm to any network or other devices to which your computer is connected.

Have a firewall enabled:

A firewall is a layer of security that decides what traffic is and isn't allowed to enter your computer on a network. Generally, firewalls let good traffic through, while keeping hackers, and malware out.

Protect yourself with a password or PIN:

A password or PIN defends against people who have physical access to your machine by locking them out of the software on the device. Passwords and PINs should be as complex as possible and use letters, symbols and number combinations that are not common nor identify you in any way.

Automatically lock your screen after inactivity:

Setting the device to 'lock' the screen after a period of inactivity defends against people who have physical access to your machine. It is easy to forget to lock your computer -- an inactivity lock prevents someone physically accessing your device without your knowledge or permissions.

THE UNIVERSITY OF CHICAGO | **Information Technology Services**