Epidemiology Department Information Security Guidelines
(Based upon UNC Information Security Policies)
Version 3/22/2011

Quick Checklist (Details follow this sheet)

- □ Study teams (PI, project manager, programmer, research associates and student-employees) should confer to review policies and plans to address.
- □ If any of your data can be considered sensitive information, determine where it is stored.
  - If on a laptop, external hard-drive, other mobile device, or desktop:
    - Obtain written approval from your project P.I. and the department chair using the form found at the end of this document.
    - For laptops and other mobile devices, encrypt with free PGP Whole Disk Encryption software. PGP WDE is currently not required by policy for desktops, but it is recommended.
    - Install SEP-11 anti-virus software.
    - Monthly vulnerability scanning using Qualys software will be activated by the department.
    - Provide data backup.
  - If on a server:
    - File encryption is currently not required by policy, but it is recommended. Consider implementing PGP NetShare to automatically encrypt your file folders, or use some other encryption technique for individual files. PGP NetShare is not covered under the University’s free distribution, but our department is taking steps to purchase a limited number of licenses.
    - Limit folder access to specific ONYENs on a strict need-to-know basis.
    - If currently using AFS storage (commonly known as I: or H: drives), make plans to relocate the sensitive information to another storage option.
  - If on a non-University owned machine:
    - While current UNC policy has a technical loophole allowing it if the machine is “managed” by UNC (e.g. installing PGP WDE), it is considered an extremely high risk behavior and thus strongly discouraged.
    - If you accept the increased risks, then follow the checklist requirements for laptops found above.
- □ Provide for physical security of the device (e.g. locked personal office, laptops stowed in locked cabinets, and/or use cables that are provided by the department.)
- □ Get in the habit of using SAS encryption techniques for your datasets.
- □ Obtain an encryption utility such as PGP or Winzip.
- □ If you use flash drives to transfer sensitive data, use only the IronKey brand which offers preformatted encrypted protection. The department has acquired a limited amount for free distribution.
- □ Set your computer screen to automatically lock after a few minutes of inactivity.
- □ Archive unused data to the Carolina Digital Repository or Mass Storage.
- □ Purge old data that does not warrant archiving.
- □ Databases, datasets, or other files with Social Security Numbers must be encrypted, no exceptions.
- □ Regularly run software to detect spyware/malware.
- □ Consider completing on-line training offered by UNC on HIPAA and information security.
- □ Promote and encourage good security habits amongst your team. Enable a culture where data security is in the forefront.
- □ Read through the attached guidelines for more details on these and other best practices.

UNC Information Security policies were established by the University on 7/2/2010. The policies can be found at http://its.unc.edu/ITS/about_its/its_policies/index.htm.

The following guidelines do not substitute for the information contained within those UNC policies, but rather supplement and clarify best practices on some of the more important topics contained within each University policy. In some areas, Epid designated best practices may go beyond the minimum amount required by UNC policy.

Sensitive Information includes all data, in its original and duplicate form, which contains:

- "Personal Information," as defined by the North Carolina Identity Theft Protection Act of 2005,
- "Protected Health Information" as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA),
- Student "education records," as defined by the Family Educational Rights and Privacy Act (FERPA),
- "Customer record information," as defined by the Gramm Leach Bliley Act (GLBA),
- "Card holder data," as defined by the Payment Card Industry (PCI) Data Security Standard,
- Confidential "personnel information," as defined by the State Personnel Act, and
- Information that is deemed to be confidential in accordance with the North Carolina Public Records Act.

Sensitive information also includes any information that is protected by University policy from unauthorized access. This information must be restricted to those with a legitimate business need for access. Examples of sensitive information may include, but are not limited to, research data, public safety information, financial donor information, information concerning select agents, system access passwords, information security records, and information file encryption keys.

http://help.unc.edu/6475 Definition of Sensitive Data
http://help.unc.edu/6604 Legal References for Sensitive Data
http://help.unc.edu/6446 Securing Sensitive Data

If you are uncertain as to whether or not your specific case qualifies as sensitive information, contact your PI for assistance. If it is still unclear, then you should contact the Information Security Office (ISO) for an official determination at security@unc.edu or 445-9393. Through collaboration with you and possibly the Office of University Counsel, the ISO can advise you of your obligations.

We understand that maintaining proper data security can be challenging, so we encourage you to **contact the Epid IS Support team with any questions you might have by submitting a Remedy help ticket** (https://www.unc.edu/ar-bin/websub/index.pl?page=main&def1=SPH-Epidemiology).
We can help analyze your situation, explain options, and recommend an approach that will meet University regulations.

What we are facing: Every day, the University experiences 30,000 attempted hacks. Every week, University employees report lost or stolen laptops. Last year, three University departments reported physical break-ins where desktop machines were stolen. The decentralized nature of our University structure and the perceived value of our data make the University a prime target in the eyes of criminals. There is limited University funding to properly address the scope of this challenge. Each University department has had Information Security Liaisons (ISL) appointed by the Chair or Dean that have been tasked to work with the ISO. These ISLs will be meeting monthly to further learn and disseminate UNC advancements on the overall topic of data security. As such, this is a living document that will keep adapting as new technologies, ideas, and University policy changes warrant.

UNC Information Security Policy

http://its.unc.edu/ccm/groups/public/@its/documents/content/ccm1_033440.pdf

- Consider storing your data on a UNC authorized server that is in compliance with UNC information security policies. Relatively speaking, server storage allows for the best possible data protection by experts in network administration, physical security, data security, system patch management, vulnerability monitoring, and backup procedures. Epid will not establish project servers within the department. We will continue to rely upon SPH, ITS, and other authorized groups within UNC to provide this critical service.

Current University server storage for sensitive information is in transition due to the upheaval caused by the CMR data breach at the School of Medicine. In the interim, Epid is one of two groups on campus working with the ISO to implement PGP NetShare software to encrypt our server data. PGP NetShare works behind the scenes to encrypt your server files automatically. While current UNC policy does not mandate encryption of server data, it is a University recommendation. Seek help from Epid IS so that you better understand your options for server storage.

If you have sensitive info on AFS (ITS servers commonly referred to as the I: drive or H: drive), you'll need to take action. **ITS does not want sensitive data stored on AFS**. While the server itself is considered secure, the older technology of AFS does not meet the strict regulations required for auditing access in case of breach. You should make plans to utilize another storage option for sensitive files. In the meantime, protect with encryption.

Server file folders are required to be configured to only allow access by authorized ONYENS. Generally, this is done at setup when you request a server folder to be created and you provide specific ONYENS other than your own to have access. Be aware that an ONYEN granted access to a folder at a higher level will most likely have access to sub folders beneath that directory tree structure. Be careful of which folder you place your sensitive data in and be mindful of the ONYEN authorizations that you have granted along the directory tree structure. Epid IS, via SPH network administrators, can provide you with a list of who has access to your SPH server folders. When team members leave your project (or transfer to another UNC department or terminate employment), you must submit a help ticket request to remove their ONYEN from authorization to your folder. Failure to do so may allow them continued access to your data.

Finally, Epid is monitoring proposals by ITS that will significantly increase each employee's server storage capacity. If that initiative is funded, Epid will take action to be on the initial wave of the rollout and purchase PGP NetShare licenses to protect this data reservoir.

- It is recognized that it is not always feasible to store data on a server. You may have highly sensitive material whose protocol requires a stand-alone computer without a connection to a Local Area Network (LAN) or the Internet. Or, the volume of data that you are dealing with exceeds the server capacity allotted to you by the University. Or, you are without reliable Internet connection to a UNC server. In those and other cases, the department is required by policy to track, monitor, and protect the off-server machines where this data resides.

  Therefore, any off-server storage (e.g. laptops, desktops, external hard-drives, USB flash drives) of sensitive data requires special handling to maintain compliance with UNC policies. Users must understand that they have assumed an increased level of risk and responsibility for protecting data that is stored off-server.

  For each off-server device *used to store sensitive information,* the user is required to:

  - Obtain written approval from the project PI and department chair using the form "Authorization for Off-Server Storage of Sensitive Information" found at the end of this document. Knowing where the department's most vulnerable data lies is the first step to protecting it. The department is required by policy to maintain a written record of where this data resides and to make those records available to the ISO upon request.
  - Install PGP Whole-Disk Encryption software. While the ISO is currently only mandating PGP encryption for mobile devices, they have extended the free licenses for use on desktops as well. So, we recommend that you take advantage of the offer now for desktops as it will likely be required in the future. *Caution*: PGP WDE only protects your data from theft/loss when the device is shut down or in 'hibernate' mode. It does not protect your data when the device is on or in 'sleeping' mode, nor does it protect you from malware or vulnerabilities that are exploited remotely via viruses. PGP WDE is not a "silver bullet". Be careful that you are not lulled into a false sense of security by relying totally on PGP WDE to protect your data.
  - Install SEP-11 anti-virus software.

    - Accept monthly vulnerability scanning of the laptop/desktop which is automated and controlled behind-the-scenes by the Epid IS team using Qualys software. The department is mandated by policy to invoke this software on a monthly basis to identify vulnerabilities in the machine’s operating system which a hacker could potentially exploit. The Epid IS team will notify you of all high level alerts generated by the software and attempt to rectify them on your behalf.
    - Provide for physical security of the device (e.g. locked personal office, laptops stowed in locked cabinets, and/or with cables that are provided by the department).
    - Provide appropriate data backup. Iron Mountain is recommended.
    - Refrain from web surfing for personal use when you have sensitive data on your machine. The Internet is a prime source for infecting your machine with viruses, spyware, and malware.

- Sensitive data on the personal machines of students and employees (e.g. home computers or laptops not owned by UNC) is ***strongly discouraged***. While current UNC policy has a technical loophole allowing it if the machine is “managed” by UNC (e.g. installing PGP WDE), it is considered an extremely high risk behavior. Epid IS Support can’t effectively monitor and control personal machines to the degree expected with UNC owned machines. For example, we have no control over outside vendors that service the machine and thus have access to its contents, nor can we prevent dangerous software such as music file sharing programs from being installed that put the data at risk. Separating your personal computing needs from your work duties is advice that should be heeded.

- Sensitive data is best protected by instituting multiple barriers to access. Determined hackers can potentially make it past the initial security provided by your machine or server. ***No machine or server can be expected to be 100% fail safe.*** The CMR server breach in the fall of 2009 was a case in point. Current UNC policy only “recommends” file/folder encryption on a server, but you are strongly urged to always encrypt your sensitive data files no matter where they are stored. File encryption can be accomplished by:

    - SAS encryption of datasets. This is extremely easy to do, and should be a regular habit.

```
************************************************
*This documents how to utilize basic SAS encryption services called SASProprietary that is included
*with Base SAS software. To prevent your password from being included in your code, and thus
*potentially being viewed by an unauthorized person, submit this statement that denotes your password
*prior to executing your SAS program. The macro variable will be in effect during your interactive SAS
*session.
************************************************;

%let mypswd = zgb213#dm;

************************************************
* SAS program example using the technique.
************************************************;
libname sasperm “M:\doejohn\myproject\data”;

* Save your dataset permanently in the secure file server folder with password & encryption protection;
data sasperm.patients (pw=&mypswd encrypt=yes);
set indata;
* do some processing;
run;

* Any reference to that protected dataset now requires the password;
proc print data=sasperm.patients (pw=&mypswd);
run;
```

    - Winzip is a popular utility used by the majority of Epid personnel. In addition to its main usage of file compression, Winzip also offers encryption. How to encrypt varies depending upon which version you have, but in general, look on the main menu or home tab for a checkbox option called “Encrypt”. You’ll know you’ve found it if you’re then prompted to provide an encryption password.

- PGP-Zip. The PGP brand of encryption software is fast becoming a standard within the University. The PGP WDE software also contains the ability to encrypt individual files with PGP-Zip. PGP WDE licenses are currently provided for free by the University.
- PGP-Netshare software offers automatic encryption of server side file folder contents. It is worth considering for the convenience and peace of mind it offers. Although this software is separate from PGP WDE and not part of the University’s free distribution, our department is taking steps to purchase licenses for distribution.

Consider the following basic example of instituting three barriers to access:

1. Keep data on the server which, relatively speaking, provides the most comprehensive security as offered by the services of a trained network administrator who “has your back” by monitoring for hacker activity, patching system upgrades, providing physical security, data back-up, and disaster recovery.
2. Use the SAS encryption technique to protect your datasets.
3. When finished with regular processing of your SAS datasets, use Winzip or another compression utility to compact and encrypt the files with yet a different password.

To get at your data, a hacker must then successfully pick the lock to your ONYEN protected server file folder, the Winzip password, and then the SAS dataset password.

Contact Epid IS or the ISO via a Remedy help ticket for advice on file encryption techniques.

It is hoped that at some point in the near future, the University will offer more seamless solutions such as abundant, automated, encrypted server storage.

- Data archival is a major issue given the vast amounts of data generated within Epid. Two options are available to off-load your data upon project closure.

  1) Carolina Digital Repository (CDR) is managed by the University Electronic Records Archivist. It is a relatively new service that is gradually being introduced (http://cdla.unc.edu/).
  2) ITS Research Computing’s Mass Storage Tape Archival (http://help.unc.edu/6291). Although the documentation for Mass Storage indicates that it is not suitable for sensitive data, the service providers will allow it *provided that you encrypt the data before storing it on the tape.*

- No new data systems or databases may be developed that do not have unique user identification, authentication, audit trail, and inactivity timeout capabilities. Existing systems must at a minimum have password protection. Our department is actively seeking new, on-line database applications that will comply with the new policies and that can serve as our common database management system across all projects.

- Datasets, databases, or other files that contain Social Security Numbers must have this field encrypted, no exceptions.

- SEP-11 anti-virus software is required on all Epid owned machines. Epid IS will gradually be phasing in the necessary anti-virus software over time to all Epid computers (i.e. you do not need to submit a help request.) Also, the SEP-11 Home Use version is intended for use on the personal machines of faculty and staff. It is provided free of charge for UNC-Chapel Hill affiliated employees and can be downloaded from the Shareware site (shareware.unc.edu).

  Signs of Spyware:
  - You are subjected to endless pop-up windows.
  - You are redirected to web sites other than the one you typed in your browser.
  - New, unexpected toolbars appear in your web browser.
  - New, unexpected icons appear in the task tray at the bottom of your screen.
  - You browser’s home page suddenly changed.
  - The search engine your browser opens has been changed.

- Certain keys fail to work in your browser (e.g. the tab key).
- Random Windows error messages begin to appear.
- Your computer suddenly seems very slow when opening programs or processing tasks.

How you can prevent spyware from installing on your computer:

- Don’t click on links within pop-up windows.
- Choose ‘no’ when asked unexpected questions.
- Be wary of free downloadable software.
- Don’t follow links claiming to offer anti-spyware software.
- Adjust your browser preferences to limit pop-up windows and cookies.

How you can remove spyware:

- Run a full scan on your computer with your anti-virus software.
- Run a legitimate product specifically designed to remove spyware. Popular products include Lavasoft’s Ad-Aware, Webroot’s SpySweeper, PestPatrol, Malwarebytes, and Spybot Search and Destroy.

Contact Epid IS via a Remedy help ticket for advice on spyware prevention, detection, and removal.

- To securely erase sensitive data from your machine, contact Epid IS for assistance. They can utilize software such as Active KillDisk to zero out the hard drive or any partition you want deleted. Shredding of the hard disk is also available by the University for $15.

- All Epid employees and other personnel (students, contractors) exposed to sensitive data are required to take CITI training. (https://www.citiprogram.org/)

- All Epid IT personnel are required to take annual HIPAA training (http://blackboard.unc.edu/) as well as UNC’s Information Security training (https://itsapps.unc.edu/ITSSelfStudy/). PI’s are strongly encouraged to have their research team members take this additional training as well.

UNC Transmission of Protected Health Information and Personal Identifying Information Policy

http://its.unc.edu/ccm/groups/public/@its/documents/content/ccm1_033439.pdf

- Access to UNC servers from off-campus requires the use of VPN software (http://help.unc.edu/2502). VPN provides the necessary encryption needed while your data is in transit. For further details see ”Off-campus Access to UNC Computers”: http://www.sph.unc.edu/epid/tech_support_6887_7051.html

- To exchange sensitive data securely either with those outside of UNC or internal employees, SoNAS software from ITS is free and satisfies the UNC policy on transmission. For further details see “SoNAS Secure Data Transfer”: http://www.sph.unc.edu/epid/tech_support_6887_7051.html

- The UNC email system allows for secure transmission (via IronPort software) to non-UNC email accounts. To take advantage of this encryption, you must type “(secure)” in the subject line of your email (without the quotes). For further instructions, see http://help.unc.edu/CCM3_020818.

  Caution: This should not be interpreted as a license to transmit sensitive data using email! This method does not require authentication at the receiving end, i.e. the recipient of the email can read the contents without being prompted for a password. You could potentially email the wrong person by mistake, thus triggering a mandated security incident report to be filed with the ISO! The SoNAS method of secure transmission (as noted above) is recommended over email because authentication is required on both ends.

- The encrypted data transfer methods described above only protect the data as it is sent “over the wire” during transmission from point A to point B. It is also strongly recommended that you encrypt the specific file that you are sending as well. It is an extra layer of insurance to ensure that your recipient practices good data habits by storing your received file on their system in an encrypted fashion.

- Inbound files received from third parties (e.g. vendors, collaborators, colleagues) that contain sensitive data must have been transmitted to you via a secure method and subsequently stored at UNC in an encrypted fashion. The third party should be notified to correct any unsecured transmission as well as informed that UNC cannot accept such unsecured file transfers. Unsecured files should be destroyed.

- USB keys (aka flash drives) should be used sparingly, if at all, and with extreme caution. Sensitive data on a USB key are required to be encrypted. *The SoNAS method of secure transmission (as noted above) is recommended over USB keys.* If you still insist on using USB keys, it is strongly recommended that you purchase a special USB encryption key that is specifically designed and pre-formatted for encryption (e.g. https://www.ironkey.com/). The IronKey brand has been used successfully by Epid personnel for various projects. Use of the IronKey requires an encryption password and the contents will be automatically destroyed upon successive invalid passwords. IronKey can be purchased via a Remedy ticket to our Epid IS team, though currently the department has purchased a limited amount for free distribution. They come in all sizes and prices, and are cheap insurance given the dangers of loss and theft with these ubiquitous devices.

- Manual data exchanges: Sometimes it is not possible to exchange data electronically. Please use the following as a guideline that has been used within Epid to follow a strict federal protocol for such occasions:
  1. Use an IronKey USB (see above).
  2. Encrypt the data file (with a different password from the IronKey) that is to be added to the IronKey. This extra effort protects both you and your recipient should your recipient fail to follow good security practices after the file is transferred from the IronKey to their machine.
  3. Set the IronKey preferences to automatically destroy the contents after a certain number of failed password attempts.
  4. Use a delivery service that offers tracking (e.g. FedEx). Request a return receipt. Do not mail on a Friday where the package will sit unattended over the weekend.
  5. Call your recipient with the passwords to unlock the IronKey and your data file encryption. (Do not email the passwords.) Remind the recipient to use the same procedures in reverse for data that is to come back to you.

UNC Password Policy for General Users

http://its.unc.edu/ccm/groups/public/@its/documents/content/ccm1_033418.pdf

Create complex password choices:

- At least 8 characters
- At least 1 letter and at least one numerical digit.
- At least one special character, such as !, #, $, %, ^, etc. Do not use @ or ?
- Cannot contain all or part of your username or be one of your previous 5 passwords.

Regularly change passwords:

- Change on a Monday so you have all week to remember.
- Change all passwords at the same time.
- Use different passwords for home versus work.
- If you must write down passwords, secure them in a locked drawer or encrypt.
- Never accept the option to save your password settings.

Password protect computers and use password protected screen savers.

- All computers should have login passwords.

- Activate your screensaver and require a password to be entered before the screen unlocks. Set log in required after 10 minutes of inactivity, preferably shorter. Some Epid projects are already setting this configuration to 3 minutes.
- Lock your computer when you leave your office (on a PC, press Ctrl+Alt+Delete and select “Lock Computer” on a Mac).

Never share your ONYEN and password, nor utilize someone else’s.

To help manage your multitude of passwords, consider KeePass software at http://keepass.info/.
KeePass is a free open source password manager, which helps you to manage your passwords in a secure way. You can put all your passwords in one database, which is locked with one master key or a key file, so you only have to remember one single master password or select the key file to unlock the whole database. The databases are encrypted using the best and most secure encryption algorithms currently known (AES and Twofish).

Locknote is another free product that offers similar functionality to KeePass:
http://www.securityfocus.com/tools/3791

UNC Information Security Liaison (ISL) Policy

http://its.unc.edu/ccm/groups/public/@its/documents/content/ccm1_033420.pdf

- The department ISL must report security incidents to the ISO consistent with the Incident Management Policy.

- The department ISL must track and monitor machines that store sensitive information.

- The department ISL must record users who handle sensitive data and ensure that the necessary signatory authorizations have been provided by the dean or department chair. This information is subject to review at any time by the ISO.

- Epid’s primary ISL is David Kleckner. Spencer Gee is the designated backup.

UNC Vulnerability Management Policy

http://its.unc.edu/ccm/groups/public/@its/documents/content/ccm1_033421.pdf

- Machines housing sensitive data (both laptops and desktops) will automatically be monitored monthly by Epid IS staff via Qualys vulnerability software. This monitoring is done behind-the-scenes, and the user should not discern any noticeable impact. The Qualys software seeks to identify vulnerabilities in the operating system that a hacker could potentially exploit. Epid IS staff will notify users and attempt to repair the damage for those machines that have generated high level security warnings.

UNC Incident Management Policy

http://its.unc.edu/ccm/groups/public/@its/documents/content/ccm1_033423.pdf

- If at any time you suspect a system or machine which hosts or processes sensitive data is compromised, *stop* any further use and immediately submit a critical level Remedy help ticket to ITS-Security. You may also call the UNC Help Desk at 962-HELP. Your immediate response may be the difference in notification situations. If you don’t stop and notify the ISO, you may unwittingly continue to update the internal date/time stamps that are maintained on data files by the operating system, thus making it extremely difficult for authorities to determine if your data has been compromised by outside hackers and thus warrant a costly and wide distribution of notification to potentially impacted parties.

- To report other security incidents contact the Epid department ISLs (David Kleckner or Spencer Gee), notify the ISO at security@unc.edu, or call the UNC Help desk at 962-HELP.

- After reporting a suspected security incident, you should anticipate the following requests from the ISO:
  - What types and amounts of sensitive data are in danger?
  - What business critical services would be impacted by isolation and/or confiscation of the affected machine for further forensic investigation?

- UNC policy requires each department to maintain a lengthy written procedure on how to handle security incidents. Those that care to read further should select the link “Data Security Incident Management Guide” found here: http://www.sph.unc.edu/epid/tech_support_6887_7051.html

UNC Email Address Policy

http://its.unc.edu/ccm/groups/public/@its/documents/content/ccm3_025561.pdf

- All faculty, staff, and student-employees must use university owned, managed, or approved email addresses for all work-related email correspondence.

- All faculty, staff, and student-employees must maintain a university email address in the campus directory. Campus directory listings of an external email address (e.g. @yahoo.com or @gmail.com) are not permitted.

- Faculty, staff, and student-employees may not automatically forward email from campus email systems to external non-university managed email systems (such as Yahoo, Gmail, or Hotmail). It is the auto-forward feature that is banned, not the manual forwarding of messages.

Authorization for Off-Server Storage of Sensitive Information

Requestor's Name: ______________________________________ **Date**: _____ / _____ /__________

Type of sensitive information to be stored:
□Personal Information, as defined by the North Carolina Identity Theft Protection Act of 2005
□Protected Health Information, as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
□Student education records, as defined by the Family Educational Rights and Privacy Act (FERPA)
□Customer record information, as defined by the Gramm Leach Bliley Act (GLBA)
□Card holder data, as defined by the Payment Card Industry (PCI) Data Security Standard
□Confidential personnel information, as defined by the State Personnel Act
□Information that is deemed to be confidential in accordance with the North Carolina Public Records Act

Where will the sensitive information be stored?
□Laptop
□Desktop
□External hard drive
□Other, describe: ____

Is it a UNC owned device?
□Yes
□No, describe: ____

Please describe the circumstances for storing sensitive information off-server.:

____

____

____

____

____

____

____

____

I accept responsibility for complying with UNC Information Security policies. I understand that help is available to me from the Information Security Office and Epid IS.

Requestor's Signature: ____ **Date**: ____/____/________

Approved by Project P.I.: ____ ____/____/________

Approved by Dean or Epid Dept. Chair: ____ ____/____/________

Required software installations by Epid IS on the machine housing sensitive information:
PGP Whole Disk Encryption: ____ ____/____/________
SEP-11 anti-virus: ____ ____/____/________
Qualys vulnerability monitoring: ____ ____/____/________