Outagamie Waupaca Library System

OWLS Information Security Policy

Adopted Feb 16, 2017; Revised: April 16, 2020; March 16, 2023

Contents

OWLS Information Security Policy and Supporting Procedures

Overview

This policy and supporting procedures are designed to provide OWLS with a documented and formalized information security policy in accordance with Requirement 12.1 of the PCI DSS standards. Additionally, this policy also serves as the organization's primary, enterprise-wide information security manual. Compliance with the stated policy and supporting procedures helps ensure the safety and security of all OWLS system components within the cardholder data environment and any other environments deemed applicable.

Implementation

This comprehensive policy document is to be implemented immediately along with all relevant and applicable procedures. Additionally, this policy is to be evaluated by OWLS staff on an annual basis for ensuring its adequacy and relevancy regarding OWLS's needs and goals.

Scope

This policy and supporting procedures encompass all system components within the cardholder data environment that are owned, operated, maintained, and controlled by OWLS and all other system components, both internally and externally, that interact with these systems, and all other relevant systems.

- Internal system components are those owned, operated, maintained, and controlled by OWLS and include all network devices (firewalls, routers, switches, load balancers, other network devices), servers (both physical and virtual servers, along with the operating systems and applications that reside on them) and any other system components deemed in scope.
- External system components are those owned, operated, maintained, and controlled by any entity other than OWLS, but for which these very resources may impact the confidentiality, integrity, and availability (CIA) and overall security of the cardholder data environment and any other environments deemed applicable.
- Please note that when referencing the term "system component(s)" or "system resource(s)" it implies the following: Any network component, server, or application included in or connected to the cardholder data environment or any other relevant environment deemed in-scope for purposes of information security.

Roles and Responsibilities

- **Computer Network Manager:** Responsibilities include implementing the baseline configuration standards for all in-scope system components. This requires obtaining a current and accurate asset inventory of all such systems, assessing their initial posture with the stated baseline, and undertaking the necessary configurations.

  Furthermore, this individual is also responsible for monitoring compliance with the stated baseline configuration standards, reporting to the Director all instances of non-compliance and efforts undertaken to correct such issues. Other duties include:

  - Assessing and analyzing baseline configuration standards for ensuring they meet the intent and rigor for the overall safety and security (both logically and physically) of critical system components.

- Ensuring the asset inventory for all in-scope system components is in fact kept current and accurate.
- Ensuring that network topology documents are also kept current and accurate.
- Facilitating requests for validation of baseline configurations for purposes of regulatory compliance assessments and audits – such as those for PCI compliance.
- Continuous learning for purposes of maintaining an acceptable level of information security expertise necessary for configuration management.

Additional duties of the Computer Network Manager include the following:

- Establishing networking environment by designing system configuration; directing system installation; defining, documenting, and enforcing system standards.
- Optimizing network performance by monitoring performance; troubleshooting network problems and outages; scheduling upgrades; collaborating with network architects on network optimization.
- Updating job knowledge by participating in educational opportunities; reading professional publications; maintaining personal networks; participating in professional organizations.
- Securing network system by establishing and enforcing policies; defining and monitoring access.
- Reporting network operational status by gathering, prioritizing information; managing projects.

- **OWLS, NFLS and member library staff:** Responsibilities include adhering to the organization's information security policies, procedures, practices, and not undertaking any measure to alter such standards on any such OWLS system components. Additionally, staff are to report instances of non-compliance to library or system management. Staff – while undertaking day-to-day operations – may also notice issues that could impede the safety and security of OWLS system components and are to also report such issues to library or system management.
- **Vendors, Contractors, Other Third-Party Entities:** Responsibilities for such individuals and organization are much like those stated for staff: adhering to the organization's information security policies, procedures, practices, and not undertaking any measure to alter such standards on any such system components.

Definitions

Cyber Security

Here's one definition of cyber security:

> *The various measures - such as the enforcement of policies, and the enactment of necessary processes and related procedures - for helping ensure the confidentiality, integrity, and availability (CIA) of information systems from malicious attempts in compromising system security that can ultimately disrupt, disable, destroy, and harm an organization's system resources.*

It's about putting in place measures for protecting one's information systems from the ever-growing threats in today's cyber world. There's a tremendous effort currently underway by organizations all around the world, publicly traded companies, local, state, and federal agencies – and many other entities – to ensure the safety and security of their entire information systems landscape.

Data Security Breaches

A data security breach is defined as the intentional or unintentional release of secure information into an untrusted environment. Many of the most well-known data security breaches are a direct result of carelessness by individuals along with failing to update critical security measures. Numerous laws, regulations, and industry specific mandates requires organizations to not only put in place comprehensive measures for mitigating data security breaches, but also requirements for notifying individuals of such breaches.

As a staff member in an OWLSnet organization, you'll ultimately come across information deemed highly sensitive and confidential, so remember to ask yourself some basic questions, such as "Do I have the right to access this information, is the information being stored securely from unauthorized parties", and many other basic security questions. It's also important to note the different types of data security breaches, which - according to privacyrights.org - generally consist of the following:

- **Unintended disclosure** - Sensitive information posted publicly on a website, mishandled or sent to the wrong party via email or any other type of end-user messaging technology.
- **Hacking or malware** - Electronic entry by an outside party, malware and spyware.
- **Payment Card Fraud** - Fraud involving debit and credit cards that is not accomplished via hacking. For example, skimming devices at point-of-service terminals.
- **Insider** - Someone with legitimate access intentionally breaches information - such as an employee or contractor.
- **Physical loss** - Lost, discarded or stolen non-electronic records, such as paper documents
- **Portable device** - Lost, discarded or stolen laptop, smartphone, tablet, portable memory device, CD, hard drive, data tape, etc.
- **Stationary device** - Lost, discarded or stolen stationary electronic device such as a computer or server not designed for mobility.
- **Unknown** - Anything outside of the above listed categories.

Our reliance on information technology - though plentiful with benefits - also brings large risk and even larger responsibilities by employees for being aware of any perceived or actual instances of intentional or unintentional release of secure information into an untrusted environment. Data security breaches are costly, extremely damaging, with long-lasting negative effects. Again, if you see something, say something - immediately!

Personally Identifiable Information (PII)

The ability to ensure the safety and security of PII for OWLS is highly dependent upon understanding what PII is. For our organizations, PII generally consists of the following:

- Full name, with all middle names (especially if the name is not common), address, date of birth, telephone numbers.
- Any part of an individual's name that is stored or displayed in conjunction with any of the subsequent listings of data and information deemed personally identifiable
- National or state identification information, such as passports, visas, permanent residence cards, voting information, social security number (United States), driver's license or any other type of unique identifier used on a national level, state or local level.
- Digital Identifiers, such as IP addresses, usernames, passwords, etc.
- Financial and Accounting records, such as banking, mortgage, revolving debt and tax information, along with credit and debit cards.
- Any other information deemed PII, but not listed above

In summary, PII consists of both the ***data and information*** that is unique to an individual and the ***source*** of the applicable data and information. For example, a social security number is the "data and information" of PII and the social security card or anywhere the number is found, imprinted, stored, or kept is the "source" of PII.

OWLS servers and network equipment

Provisioning and Hardening

All OWLS system components are to be properly provisioned, hardened, secured, and locked down for ensuring their confidentiality, integrity, and availability (CIA). The following provisioning and hardening procedures will be applied as necessary when deploying system components onto OWLS's network:

- Vendor-supplied default settings are changed.
- All unnecessary accounts are eliminated.
- Only necessary and secure services, protocols and other essential services are enabled as needed for functionality.
- All unnecessary functionality is effectively removed.
- All system security parameters are appropriately configured.

The provisioning and hardening process will be undertaken by the Computer Network Manager with assistance from other IT personnel as needed.

Physical and Environmental Security

OWLS will implement necessary physical security controls for all OWLS network components. Network components will be stored in a server room that is secured and monitored at all times and whereby only authorized personnel have physical access to the specified system components. The following controls apply to the server room:

- Adequately protect all system components.
- Kept locked at all times. Access will be by means of a keypad lock, and only authorized personnel will have codes to unlock the door.
- Security alarms that are active during non-business hours, with alarm notifications directly answered by a third-party security service or local police force.
- Temperature monitoring and notification.
- Appropriate fire detection and suppression elements, along with fire extinguishers placed in mission critical areas.
- Appropriate environmental conditioning, including air conditioning, dehumidifying, and heating.
- Appropriate power protection devices for ensuring a continued, balanced load of power to the specified system resource, thus mitigating power surges and spikes.

Access Rights to OWLS system components

Access rights to OWLS system components are limited to authorized personnel only.

Additionally, staff with elevated and/or superuser privileges, such as the Director, Computer Network Manager, OWLSnet Manager, Computer Technology Coordinator, and Computer Technician are responsible for ensuring access rights for staff are commensurate with roles and responsibilities within OWLS.

When possible, functions (such as read, write, edit, etc.) are not grouped together and staff and administrators are not granted access to multiple functions. By effectively separating access rights to system components whereby only authorized individuals have access to the minimum rights needed to perform their respective duties, OWLS is adhering to the concept of "least privileges", a well-known and best practices rule within information technology.

Passwords used by all staff must meet or exceed all stated OWLS policies for password complexity requirements. Further, OWLS staff are required to use a password manager with multifactor authentication enabled for their master password.

Password Parameters

- Password parameters are set to require passwords to be at least twelve characters long.
- Password parameters are set to require passwords to contain both numeric and alphabetic characters.
- Passwords for new staff are set to a unique value.

Patch Management

On a quarterly basis, the Computer Network Manager will evaluate the need and risk for installing new patches or updates on all OWLS servers.

OWLS will follow recommendations from the ILS (Integrated Library System) vendors for servers supporting the Integrated Library System and Discovery Layer.

Backup and Storage

Data backup and storage procedures for OWLS system components are to be initiated by the Computer Network Manager, OWLSnet Manager, or Web and Marketing Coordinator.

A full (tape) backup is performed on the OWLSDNS4 (physical) server M-F each week. Our VMware virtual servers are backed up on tape using the full backup option every Sunday. Incremental backups of the virtual servers are kept on the Computer Network Manager's PC during the balance of the week. Internal server backups have a 3-week retention period using 3 sets of backup tapes. The Computer Network Manager receives daily emailed notifications of all DNS and virtual server backups.

Office 365 files and email are backed up daily using a third-party cloud-to-cloud service.

The Web and Marketing Coordinator ensures that all OWLS managed websites are regularly updated and fully functional. OWLS websites have a daily backup schedule coordinated with the managed web hosting solution. The Web and Marketing Coordinator receives notification of all web server backups.

- The entire web server is backed up daily using Acronis backup and recovery software.
- The Web and Marketing Coordinator views the current backups weekly and verifies that they are working properly.
- The Web and Marketing Coordinator has alerts set that in the event of a backup failure they will be immediately notified.
- Backups are stored in a cloud server managed by the web hosting provider.
- Additionally, for WordPress websites, OWLS uses UpdraftPlus, a general purpose backup solution, to back up website files, database, and configuration files.
- The managed web hosting solution aids in any recovery process to ensure websites can be restored quickly and efficiently in the event of a disaster.

Our ILS and Discovery platforms are hosted, and backups are managed by the respective vendors.

Incident responses are determined by the Computer Network Manager, OWLSnet Manager, or Web and Marketing Coordinator with consultation from other staff and the Integrated Library System (ILS) vendor's support team as necessary. When data has been compromised due to any number of reasons, appropriate restore procedures will be enacted that allow for complete, accurate, and timely restoration of the data itself.

Encryption

Whenever possible connecting to remote network resources (i.e. switches, routers, servers) should be done using an encrypted connection. SSL layer encryption is required for command line access to internal servers. Additionally, computers used to access the ILS remotely, via wireless access, will have their hard drives encrypted.

Data Retention and Disposal

It is company policy to limit data storage amount and retention time to that which is required for legal, regulatory and business requirements. OWLS has adopted and follows the Record Retention Schedule for Wisconsin's Public Libraries and Public Library Systems adopted by the Wisconsin Public records Board on June 12, 2017.

The following methods are to be utilized for both hard copy and electronic data:

- Purging and deleting data from all system components. This can be done by utilizing a secure wipe program in accordance with industry-accepted standards for secure deletion.

For electronic media stored on system components that are no longer in use, data is to be disposed of through disintegration, shredding, incineration by a licensed incinerator or pulverization.

Incident Response Plan

OWLS has many security procedures in place to prevent security breaches, including properly configured computers, servers, and networks. However, no plan is foolproof, so OWLS is prepared to act in the event of a security breach.

In the event that a security breach is discovered or suspected, the person who discovers the incident should call the OWLS office. This person may be a staff member of an OWLSnet member library, or a staff member of OWLS or NFLS. If the incident occurs outside of office hours, OWLS system staff should be contacted using the after-hours call list distributed to all member libraries and system staff.

Examples of potential security breaches include: Theft or loss of computers and laptops, flash drives, electronic media or paper files that include PII (personally identifiable information), insecure storage or transmission of PII and other sensitive information, servers or passwords hacked or revealed, computers or servers infected with a virus or other malware, or insecure disposal or re-use of devices with sensitive information.

The OWLS employee who takes the call will immediately contact the Computer Network Manager, OWLSnet Manager, Web and Marketing Coordinator, and OWLS Director. One of these individuals will start the OWLS Incident Response Form, which will be followed through until the incident is complete.

Actual responses to the security breach will depend on the exact nature of the breach. The management of OWLS will immediately act to stop any continued breach from taking place. This may include taking services or servers offline to preserve data and prevent the problem from continuing.

If it is determined that a security breach is likely, OWLS staff will notify the cyber security insurance company. If necessary, OWLS will rebuild, reconfigure or use backup media to restore processes to a pre-breach status.

After the incident is complete, OWLS will review the incident response and determine what, if any changes should be made to existing security practices and incident response practices.

NFLS and OWLSnet member library staff will be informed of the status of the reported security breach, the outcome and any changes that result from the incident evaluation.

Disaster Recovery

OWLS has a service disruption procedure in place. OWLS will work on implementing a more comprehensive Disaster Recovery Plan in 2023. In the meantime, OWLS will continue to follow agreed upon practices of having full backups for all critical system components.

Asset Inventory

OWLS will identify all applicable unique identifiers and necessary data elements for successfully tracking and managing the OWLS servers and network equipment. At a minimum, the following elements will be used for asset inventory, when applicable:

- Type of system resource – Network devices (firewalls, routers, switches, load balancers, etc.), Servers (physical and or/logical, and the underlying operating systems and applications residing on such servers).
- Version number or application type
- Primary function
- Physical element: A stand-alone product, or a virtual element, such as an instance, etc.
- Internal hostname
- Name of product or solution (such as the vendor purchased from)
- Serial number some other type of non-hostname identification element
- IP address
- Physical location
- Logical location
- Party or parties responsible for system administration
- Detailed listing of any regulatory compliance mandates, such as those for PCI compliance.
- Detailed listing of any solutions configured onto or supporting the system resource – if applicable, such as the following:
    - Audit trails and logging
    - Anti-virus
    - Other

Remote Access

All access to OWLS system components initiated outside the organization's trusted network infrastructure is to be considered "remote access", and as such, only approved protocols are to be used for ensuring that a trusted connection is initiated, established and maintained. Specifically, all staff members are to utilize approved technologies, such as IPSec (e.g. Splashtop) and/or SSL Virtual Private Networks (VPN) for remote access, along with additional supporting measures as appropriate, such as Secure Shell (SSH).

Additionally, all PCs (both company and employee-owned) are to have current, up-to-date anti-virus software installed, while also utilizing any other malware utilities as needed for protecting the PCs and the information traversing to and

from the remote access connection. This may also include the use of personal firewall software, along with enhanced operating system settings on the applicable PCs.

Wireless Security

Most of the OWLSnet wireless networks are publicly accessible, by design.

Implementing and maintaining a WLAN requires adherence to the following stated guidelines for ensuring the safety and security of the wireless platform itself.

- **Secure Deployment:** All WLAN devices and supporting resources, such as wireless access points, and other network devices, are to be positioned in a manner for discouraging unauthorized physical access and modification. Additionally, they are to be secured with approved fixtures for mitigating any unnecessary movement. Additionally, the publicly accessible LibraryGuest WLAN platforms are to be logically segregated from the library wired networks, which can be achieved by utilizing firewalls, VLANS and other access control methods.
- **Asset Inventory:** Once all WLAN devices are safely secured, a complete asset inventory is to be taken, documenting all necessary information, such as physical location, and corresponding unique identifiers (i.e., hostnames, serial numbers, etc.). This is handled by the wireless management dashboard.
- **Configuration of Wireless Access Points:** The following measures are to be undertaken regarding WLAN platforms:
    - All non-public SSIDs will use a "closed network" concept, whereby the SSID is actually not broadcasted (if allowable), rather, it must be entered into the client application.
    - All non-public WLAN SSIDs will use the strongest encryption algorithm currently available (WPA2), and use other forms of encryption as needed, such as VPN, SSL | TLS, etc.
    - Protect all sensitive wireless access points information, such as administrator passwords, SSID password, keys, etc. with approved security measures.
    - Enable logging features and ensure that all logs and audit trails are sent to a remote logging server and retained as necessary (i.e., regulatory compliance laws, etc.).
    - At the discretion of the member library, public access to the LibraryGuest SSID can be disabled during non-business hours.

Employee Separation Process

OWLS will follow the Employee Separation Checklist when staff leave OWLS. A modified version of this form will also be used to remove access to OWLSnet computers and services when NFLS and OWLSnet member library staff leave employment.

OWLSnet PC security

Malware

Malicious software (malware) poses a critical security threat to OWLS system components, so OWLS has taken measures to protect against viruses, worms, spyware, adware, keyloggers, rootkits, trojan horses, ransomware, and many other forms of harmful code and scripts.

OWLS will deploy anti-virus (AV) solutions on all applicable system components and OWLSnet PCs. OWLS will strive to install the latest version of the antivirus software, enabled for automatic updates and configured for conducting periodic

scans as necessary. Because strong and comprehensive malware measures are not just limited to the use of AV, additional tools are to be employed as necessary for eliminating all other associated threats, such as those discussed above. The seriousness of malware and its growing frequency of attacks within organizations require that all IT personnel within OWLS stay abreast of useful tools and programs that are beneficial in combating harmful code and scripts.

Software updates

OWLSnet IT staff will work with staff at system offices and member libraries to keep software supported by OWLSnet (Microsoft operating system, antivirus, PC protection) up-to-date.

Public computers

OWLSnet installs software intended to protect public computers from changes to initial configuration and infection by malware, intended to protect the computer, other devices on the local area network and the wide area network. OWLS and NFLS member staff will investigate and work with the software vendor to correct any problems with this software that allows changes of any kind to the initial configuration.

Staff Responsibilities

Email Guidelines, Responsibilities and Acceptable Use

- The use of OWLSnet email resources is to be used primarily for official library purposes. While email is often used to communicate with friends, family members and other non-professional acquaintances, it is advised and encouraged to limit the extent of OWLSnet email resources for interaction and communication with these respective parties. Communication with friends, family members and other non-professional acquaintances should be conducted with the use of a personal, non-OWLS or -NFLS email address.
- Staff are to protect the privacy of their email accounts, which includes safeguarding passwords at all times and not allowing passwords to be viewed and copied by any other individual.
- Staff are to have their access rights permanently revoked from all computing systems that allow for access to email accounts after their employment is complete. This includes the disabling of email accounts and passwords for any user no longer employed by OWLS, NFLS or any OWLSnet member library. Terminated users will not be allowed to have any e-mails forwarded to them once they have been terminated.

Directors may request that after a change of password, email accounts either remain accessible to current staff or are forwarded to current staff for up to three months. Under special circumstances these email accounts may be accessible or forwarded for up to 6 months. The following activities are considered **unacceptable** by staff:

- Any activity resulting from the use of OWLSnet email resources that may potentially compromise the organization's network infrastructure, cause harm to other related systems, cause harm or pose a significant financial, operational, or business threat to the organization because of inappropriate and unacceptable use of email.

Internet Guidelines, Responsibilities and Acceptable Use

OWLS has established the following general guidelines, responsibilities, and acceptable uses for the internet as described below.

- When downloading content from the Internet, all files must be scanned with appropriate anti-virus software. OWLSnet antivirus software is configured to scan all downloaded files.
- The use of OWLSnet Internet resources is to be used primarily for official business purposes only. While the use of the Internet is often used to communicate with friends, family members and other non-professional acquaintances, it is advised and encouraged to limit the extent of OWLS Internet resources for interaction and

communication with these respective parties. Thus, communication with friends, family members and other non-professional acquaintances should be conducted with the use of a personal, non-OWLSnet Internet resources, primarily outside of normal business hours.

- OWLS reserves the right, without notice, to monitor all Internet activity as needed.
- Staff are to have their access rights permanently revoked from all computing systems that allow for access to Internet resources once their employment is complete. This includes the disabling of all accounts and passwords for any user no longer employed by OWLS, NFLS or any OWLSnet member library.

The following activities are considered **unacceptable** by staff:

- Any activity resulting from the use of OWLSnet Internet resources that may potentially compromise the organization's network infrastructure, cause harm to other related systems, cause harm or pose a significant financial, operational, or business threat to the organization because of inappropriate and unacceptable use of OWLS Internet resources.

Network Guidelines, Responsibilities and Acceptable Use

[Please refer to the OWLSnet Network Connection Policy.]

Attach only devices approved by OWLS to the OWLSnet network. Users shall not inter-connect OWLSnet with any other network without the consent of OWLS.

Securing your PC

Protecting your PC area – specifically your desktop computer and other supporting devices – is an important duty all employees should take very seriously. Employees spend long hours at their PCs, so it's critical to implement the following best practices:

- **It's your PC.** It should primarily be used for library purposes. Depending on your library, it may also be fine to conduct personal activities, such as checking your email, logging into online banking, or accessing social media platforms, such as Facebook and LinkedIn. Be aware that using your PC for personal uses may expose your PC to unsuspected malware.
- **Use strong passwords.** While some passwords will be given to you by system staff, it's important to make other passwords you use unique, never using information pertaining to your favorites sports team, home address, middle name, etc.
- **Lock PC when unattended.** If you step away from your computer, even briefly, lock the PC to prevent unauthorized access using the Windows Key + L shortcut.
- **Security updates.** Make sure your PC has all the required security updates for the operating system and all other applications running. This also means having anti-virus running at all times and conducting periodic scans. Additionally, the use of anti-spyware may also be required as it provides additional layers of protection, especially during Internet usage. While most of the security updates are "pushed" out and managed by I.T. personnel, at times you may need to accept these updates.
- **Don't alter security settings.** Your PC has been configured for maximum security along with performance, so do not attempt to disable or modify configuration settings to the operating system or any other applications. Doing so may increase security vulnerabilities that would ultimately allow malicious files and other harmful scripts to reside on the PC.
- **Don't install any unapproved software.** Don't download or install additional software that has not been approved by the library or system as it may contain malicious files, could consume additional resources, or is simply not professionally suitable for the work environment.

- **Removable storage devices.** They're easy-to-use, inexpensive, and a great way for transferring information, yet they're also incredibly dangerous when the wrong information is on them and in the wrong hands. Removable drives such as thumb drives, external hard drives, and other removal storage and memory devices should never contain highly sensitive and confidential information, such as Personally Identifiable Information (PII), or any other data deemed privileged. Such information should be transferred over the network using approved protocols and reside on servers owned or licensed by OWLS.
- **Use caution with email.** Be careful when opening emails from unknown parties, especially attachments. If it looks suspicious, do not open the email under any circumstances. Additionally, avoid clicking on links or banner advertisements sent to you as these often contain spyware, malware, etc.
- **Handle private information with care.** Patron privacy is a requirement of Wisconsin law, so please make every effort to protect its confidentiality and integrity. Don't divulge such information to unintended parties (either electronically, or in hard copy or in easily overheard conversation) and never leave items with confidential information (both hard copy and electronic media) unattended in public at any time (i.e., coffee shops, training seminars, conferences, etc.). It's best if all confidential patron information stays in the library.
- **Report security issues immediately.** Remember, if you see something, say something – and immediately. You have a responsibility for helping protect the organization, which means being aware of your surroundings and reporting suspicious activity to authorized personnel – immediately. From seeing a door ajar that shouldn't be to finding sensitive documents lying in a commons area, you need to take action.

Securing your laptop

Securing your laptop at all times is extremely critical, and it requires comprehensive measures regarding its physical security, while also protecting all electronic data residing on it. From travelling for meetings to connecting to open public wireless access points, your laptop is a constant target, so beware. Take the following precautions for securing what's arguably one of your most important possessions:

- **Power off in transit.** Your laptop should be powered off when in transit.
- **Use Encryption.** The use of full-disk encryption ensures that safety and security of data (i.e., user files, swap files, system files, hidden files, etc.) residing on your laptop, especially if it's stolen, lost, or misplaced.
- **Use Anti-virus.** It's one of the most fundamentally important – and often not used – security software, so make sure your laptop has anti-virus running at all times, along with its scanning at regular intervals for viruses, and that the software is current.
- **Turn on your firewall.** Blocking suspicious traffic is essential for laptop security, so turn on and "enable" your default personal firewall or an approved personal firewall software appliance, for which there are many available.
- **Use strong passwords.** When turning on your laptop, your initial password should be extremely strong, with a combination of letters, numbers, and symbols used. Once your initial password is compromised, the contents of your entire laptop (especially if you're not using full-disk encryption) can be compromised. Don't use terms and phrases for which somebody might find an association with you, such as favorite football team, home address, middle name, etc.
- **It's your laptop.** Therefore, don't let other individuals use it, especially if it's somebody you don't know. When situations arise that require it to be used by someone other than you, create a guest account for their use.
- **Secure it physically.** A good investment is a security cable with a lock for securing your laptop at a PC or any other location that requires such. They're relatively inexpensive and a great deterrent to any thief.

- **Keep a watchful eye.** Don't ever leave your laptop unattended in any public venue or location not considered safe. That means not using the coffee house phrase "can you watch my laptop for a minute as I go to the restroom", or any other similar thought process. Being vigilant and watchful at all times is a must for the safety and security of your laptop, so remember – do not leave it unattended – plain and simple. If you have to leave in your hotel room or some other location, then remove it from sight and place under a pillow, in a closet, or some other location. The best safety measure is to carry it with you at all times. If your laptop will be briefly unattended in a secure location such as your office or home, use the Windows Key + L to lock it.
- **Place your contact information somewhere visible.** Because most people are honest and trustworthy, should your laptop be stolen, misplaced or lost – and then subsequently found by a good Samaritan – you'll clearly want your name, phone number, address, and/or email visible on it. Put a sticker on the cover or back of your laptop with all your relevant contact information.
- **And if your laptop is stolen.** Laptops unfortunately do get stolen, so think and act quickly, which means reporting the theft to local authorities along with informing management (and the I.T. department) immediately.
- **Laptops with CARL installed:** These laptops should only be used by OWLSnet library staff. Because of the confidential nature of the software, library patrons and family members of library staff should not use these laptops (per the CARL in the Wild usage policy.)

Safe online practices and mobile computing

Information Security is also about understanding today's ever-growing online threats, many of which can result in serious security issues for you or your employer. We all spend large amounts of time online, for both professional and personal reasons, using laptops and portable devices, so it's important to note the following:

- **Trust, but verify.** Know who is requesting information from you, from highly sensitive and confidential patron information to your own personal information. Social engineering - tactics used to gain access and steal valuable assets - is on the rise, so be watchful and mindful at all times.
- **Enable security.** This means making sure that you have anti-virus on any computer being used to access the Internet. It also means using a username and password for protecting the contents on your laptop should it ever be lost, stolen, or misplaced.
- **Protect your physical assets.** This means not leaving your laptop, smartphone, tablet, etc. unattended for any time period. Going to the bathroom at the coffee house while leaving your notebook alone is not wise. Record the model and serial number of both work and personal laptops, in case of theft.
- **Protect your accounts.** Keep login credentials secure by using an encrypted password manager with a strong master password that you can remember and multi-factor authentication enabled. This means a clean desktop policy, one that does not contain notes lying around with login credentials. Do not reuse passwords. Change shared passwords when staff leave employment. Configure browsers not to save usernames and passwords. It's a good idea to periodically clean out your browser history (CTRL-SHIFT-DEL) to ensure no pre-populated usernames and passwords exist, especially on non-company owned desktops, laptops, and PCs.
- **Wireless Access Points.** Though they're free and easy to connect to, public Wi-Fi networks can be extremely problematic in terms of security issues, so take note of the following precautions:
    - Turn off your actual wireless connectivity when not in use.
    - Connect only to trusted Wi-Fi networks. If you aren't sure about a network that's being broadcasted, ask! If it seems suspicious, then do not connect - most Internet sessions can wait.

    - Do not use public Wi-Fi networks for conducting business activities, unless you have approved VPN and secure, remote access software on your laptop.
- **Protect wireless handheld devices.** The continued growth and use of small, mobile devices capable of sending, receiving and storing information – though highly efficient – also requires putting in place protective measures, such as the following:
    - Use PIN and/or password security parameters for accessing and unlocking your phone or tablet, as this is critical if it's ever lost, stolen or misplaced.
    - When disposing of any wireless handheld devices, ensure that all sensitive and confidential data has been removed, such as with a secure wipe program.

Software usage and licensing

While system staff update and apply critical security patches to OWLS system components, it's important that all employees also do the same for many of their devices, particularly applications used on a daily basis. Security is the first and foremost reason for applying security updates, but there are other benefits also, such as new and enhanced features, and improved performance and stability. The following are to be updated accordingly:

- Internet browsers: Updating browsers (Microsoft Edge, Mozilla Firefox, Google Chrome) is extremely important for ensuring all web pages display correctly, known security holes are eliminated, and all performance features are maximized.
- Microsoft Windows Operating Systems: Enable automatic Windows updates on your PC or laptop.
- Portable Document Format (PDF) | Adobe: Hackers can create malicious files and other executable content that can exploit Portable Document Format (PDF) protocol software, therefore it's important to click "yes" when Adobe software asks if you want to make security updates.
- Other essential applications: There's an almost endless list of applications being used today, so keep a list handy of what's on your computer, making sure to perform security updates as required for not only safety, but performance and software stability.

Please also be mindful of the following issues:

- **Use only approved software.** Only software provided or approved by the system or library should be installed on any system or library owned equipment, including your PC.
- **Downloading from the Internet.** Any software obtained from the Internet is to be considered copyright protected, which means accepting any copyright agreements. Downloaded software should also be scanned by antivirus software to help prevent dangerous or malicious code. However, antivirus scanning of installable software is limited, and will not find all malware. Therefore, be very cautious in downloading freely available software. The Internet can be an extremely dangerous forum when it comes to software as many products seem harmless, only to contain viruses that can wreak havoc on computers. Think before you start downloading *any* software online.
- **Do not duplicate software.** The licensing rights for software are strict and extremely rigid, allowing only a predetermined number of installations for a given data set. This means you are not allowed to copy or duplicate any system or library purchased software – no exceptions. U.S copyright laws – and other regulations throughout the world – often place strict guidelines on software usage, so please keep this in mind.
- **Penalties and fines.** Organizations and employees can be levied fines for improper software use. According to the U.S. Copyright Act, illegal reproduction of software is subject to civil damages up to $150,000 (Section 504(c)(1) Title 17) per title infringed, and criminal penalties, including fines of as much as $250,000 per title infringed and imprisonment of up to ten (Section 2319 (b) (2) Title 18) years.