# TABLE OF CONTENTS

FROM THE OFFICE OF INFORMATION SECURITY ................................................................. 2

PRIVACY ................................................................................................................................. 3

SECURITY STRATEGY 1 | PASSWORDS .................................................................................. 5

SECURITY STRATEGY 2 | VIRUS PROTECTION .............................................................. 6

SECURITY STRATEGY 3 | SPYWARE PROTECTION .............................................................. 6

SECURITY STRATEGY 4 | FIREWALLS ...................................................................................... 7

SECURITY STRATEGY 5 | SECURITY UPDATES ............................................................ 7

SECURITY STRATEGY 6 | COMPUTING HABITS ............................................................... 8

  Physical Security ........................................................................................................ 8

  Data Theft Techniques .......................................................................................... 9

  Email ....................................................................................................................... 11

  Protecting Data Integrity ................................................................................... 12

IT SECURITY LINKS .................................................................................................. 14

GETTING HELP ........................................................................................................ 15
FROM THE OFFICE OF INFORMATION SECURITY

The mission of Wright State University’s Department of Information Security is to support the central mission of the university by assuring the confidentiality, integrity, and availability of its information and information systems. The Department of Information Security cannot accomplish this task alone. Each and every member of the Wright State community needs to be involved.

Understanding and awareness are the keys to keeping our computing environment safe. With that in mind, Computing and Telecommunication Services has created this handbook to assist individuals in understanding what their part is and what they should be aware of concerning information security. Important information concerning passwords, virus protection, data protection, and more are discussed. The core computing practices in this handbook will serve each individual well in keeping our computing environment a safe place to conduct Wright State University’s main business focus of educating students.

Michael Natale
Manager, Information Security
PRIVACY

Wright State University is responsible for collecting, storing, and distributing very large amounts of information. Some of this information is federally legislated as private and must be protected in accordance with laws such as the Family Education Rights and Privacy Act (FERPA) of 1974 (for student records), the Gramm-Leach-Bliley Act (GLBA) of 1999 (for personal financial information), the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (for personally identifiable health information), and the Payment Card Industry Data Security Standards (PCI DSS). All members of the university have a responsibility to protect information about our students and employees from public disclosure.

Protected Information

Information that is classified as “protected” cannot be disclosed or disseminated to the public. Much of the information about our students and employees is considered protected.

Examples of protected information include (but are not limited to) the following:

- Social Security Number
- Birth date
- Credit card security code
- Encoded magnetic strip information
- Health information
- Student grades
- Gender
- Ethnicity
- Citizenship
- Citizen visa code
- Veteran and disability status
- Courses taken
- Schedule
- Test scores
- Advising records
- Educational services received
- Disciplinary actions
- Credit card numbers & expiration dates

The Wright State IT Security Policy is designed as a set of measures to protect the confidentiality, integrity and availability of sensitive data, such as those outlined above, as well as any information systems that store, process or transmit this data.

Note: Students have the right to withhold their directory information from being released by completing a "Request to Prevent Release of Directory (public) Information" form in the Registrar's Office. Once received, a confidentiality flag will be noted in the student information system to indicate that no directory information for that student is to be released. The existence of such a confidentiality flag must be confirmed before any directory (public) information is released for any student. Questions should be directed to the Registrar's Office (937-775-5588; registrar@wright.edu).

General Privacy Guidelines

All employees and users of network computing resources at Wright State University have a role in protecting the university’s information assets because their computers provide potential gateways to protected information stored on the network. Therefore, whether or not
you deal directly with protected or confidential university information, you should take the following steps to reduce the risk of data theft:

- Don’t give out information to someone you don’t know
- Identify information as “PROTECTED” on printed pages, CDs, diskettes, etc
- Take special care when posting grades (assign random numbers, and do not use any part of a Social Security Number or UID number)
- Do not leave paper documents containing protected information unattended; protect them from the view of passers-by or office visitors
- Store paper documents containing protected information in a locked location
- Do not leave keys to file drawers that contain confidential information in unlocked locations or areas that are accessible to unauthorized personnel
- Shred confidential paper documents that are no longer needed, and secure these documents until shredding occurs
- If a shredding service is employed, ensure that the service provider has clearly defined procedures in the contractual agreement that protect discarded information and that the provider is legally accountable for those procedures, with penalties in place for breach of contract
- Immediately retrieve or secure protected documents that are printed on copy machines, fax machines, and printers
- Restrict access of information and systems to people who need it to perform their jobs
- Regularly review the list of users who have access to systems that store protected information, and remove those who should no longer have the access
- Test internal processes to ensure data integrity and security
- Keep a log sheet for visitors to sign whenever they need to enter an area where sensitive information is kept and accompany visitors at all times.

**FERPA Information**

In early 2009 new FERPA regulations took effect, which prohibit the public posting of grades by any part of the student UID number in addition to any part of the Social Security Number or name. For posting grades, you may want to create and assign a unique list of randomly generated numbers/characters known and available only to you, so that the public posting of grades does not occur. Also remember not to leave exams, papers, or documents containing student information outside your office door or any area that has open access.

**Credit Card Information**

Credit card data, including the expiration date, is sensitive, confidential information which must be stored in a secure manner and destroyed when it is no longer needed. Note that the maximum retention time to keep this data is 18 months. In addition, the credit card security code and encoded magnetic stripe information should never be stored. Sensitive credit card information such as the full 16 digit card number should never be stored on a computer hard drive, network drive, or portable device such as flash drive.
SECURITY STRATEGY 1 | PASSWORDS

Passwords can be the weakest link in computer security, but can also be the front line of defense against potential data theft. Selecting a strong password, and protecting that password, is essential. Hackers frequently attempt to use password cracking tools to gain access to accounts and can do so within a matter of seconds if the password is a weak one.

Below are some tips to keep in mind when creating and using your password:

- Choose a mixture of upper and lower case letters (A-Z, a-z), numbers, and symbols
- Do not use the following symbols: % # @ ? . ,
- Use a password between 8-14 characters
- Do not use words found in a dictionary (English or foreign)
- Do not use common words or names of friends, pets, spouses, co-workers, etc
- Do not use anniversary dates, birthdates, months of the year or seasons
- Use a different password for each system (for example: Banner Admin and your CAMPUS password)
- Never save a password online and never use the “Remember Password” feature of an application or program
- Do not use your username as your password
- Do not put your password in an email message
- Do not use the same password for both a work and personal account

Check out the table below for some examples of strong and weak passwords (keep in mind that these are just examples; do not use them as your personal password):

<table>
<thead>
<tr>
<th>Weak Passwords</th>
<th>Strong Passwords</th>
</tr>
</thead>
<tbody>
<tr>
<td>summer2007</td>
<td>Summer2007</td>
</tr>
<tr>
<td>thomas1980</td>
<td>Th0m1980</td>
</tr>
<tr>
<td>abc1234</td>
<td>12ab34cd!</td>
</tr>
<tr>
<td>computer</td>
<td>c0mput3r</td>
</tr>
</tbody>
</table>

With a bit of creativity, you can make a password that is very difficult to guess, and by protecting that password, you can help ensure that personal and confidential data is protected.
SECURITY STRATEGY 2 | VIRUS PROTECTION

A computer virus is a program that implants instructions into your computer programs or storage devices that can then attack, scramble, or erase computer data. The destructiveness of viruses lies in their ability to replicate themselves and spread from system to system. It is very important to have anti-virus software running on your computer and to keep it up to date so that new viruses can be detected.

CaTS now requires that all computers connected to our network have up to date anti-virus software. For CaTS supported systems on campus (faculty and staff offices), this is done automatically. For students living in the residence halls, the software will need to be installed manually. CaTS offers a free, downloadable version of McAfee VShield for Windows at the following website: http://www.wright.edu/cats/antivirus/. You will need to login with your CAMPUS username and password in order to access this download. Also offered is a free version of the McAfee Virex anti-virus software for the Macintosh, located at the same website (http://www.wright.edu/cats/antivirus/). Installing the software from these locations will connect your anti-virus software to automatic updates.

For home users (faculty, staff, and students), anti-virus software can be downloaded for your computer at the following website: http://www.wright.edu/cats/antivirus/. You will need to login with your CAMPUS username and password in order to access this download.

SECURITY STRATEGY 3 | SPYWARE PROTECTION

DID YOU KNOW?
Unknown toolbars in your browser could indicate the presence of spyware on your computer

Spyware is any software that watches your computing activity and collects personal data without your permission. It can be hidden in programs that you download from the Internet. Once you install that program, the spyware can monitor your activity and send that information to someone else. Email addresses, web browsing habits, usernames, and passwords are just some of the data that spyware can collect. This data can then be used for identity theft, marketing, spam, and other activities. Along with the ability to steal your information, spyware also consumes large amounts of memory on your computer, making it more unstable and prone to crashing.

To reduce the amount of spyware on your Windows computer, you should have spyware protection software installed. CaTS recommends a combination of two programs: Lavasoft Ad-Aware and Spybot Search and Destroy. You can download these programs for free from our ConnectWright website, located at https://www.wright.edu/cats/cw. Once you have downloaded and installed the software, we recommend that you run a full scan of your Windows computer at least once a week. At this time, there is no known spyware protection software for the Macintosh or Linux/Unix operating systems.
SECURITY STRATEGY 4 | FIREWALLS

A firewall is a system that is designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software formats. Here at Wright State University, CaTS maintains both hardware and software perimeter firewalls for the entire campus community that control Internet traffic in and out of our network. For individual computers, personal desktop firewalls, such as Windows Firewall, should be installed to help prevent unauthorized access.

For CaTS managed computers on the Wright State network (normally defined as faculty, staff, and administrative computers), a copy of McAfee Firewall is already installed and managed through our McAfee network server. These systems should have the Windows Firewall disabled. For students living in the residence halls, a personal desktop firewall is required. The easiest and most convenient firewall to use is the Windows Firewall, but other popular programs include Zone Alarm and Tiny Firewall, which can be downloaded from the website http://www.download.com.

SECURITY STRATEGY 5 | SECURITY UPDATES

Security updates are small programs or files that patch operating systems (such as Windows) from known problems. These updates are crucial in defending against new viruses and attacks. Hackers are constantly looking for vulnerabilities in operating systems and programs, and can easily find and infiltrate a computer that has not been properly patched.

For CaTS managed computers on the Wright State network (normally defined as faculty, staff, and administrative computers), security updates are automatically installed from our update server. For students living in the residence halls, or for home users, your computer should be setup to automatically download and install critical updates. For specific directions on how to do this for your particular operating system, check out the Do IT Wright website, located at http://www.wright.edu/security/.
SECURITY STRATEGY 6 | COMPUTING HABITS

Along with security strategies such as passwords, updates, firewalls, and spyware and virus protection, your computing habits can play a very important role when it comes to securing data. One of the best computing habits to develop is storing sensitive university data on your personal H:\ drive. By storing files on your H:\ drive, you ensure that only you have access to these files. Also, by following this method, you have access to the files from any other Internet enabled computer by using the MyFiles website, located at http://myfiles.wright.edu. To read more about the many other computing habits you should be aware of to help ensure data security, check out the information below.

Physical Security

The physical security of computing resources (computers, equipment, files, etc.) is actually the first principle of good security because as long as someone can obtain physical access to your computer, he/she can gain control over it. By instituting a few simple safeguards, you can greatly limit security breaches and other unauthorized access to computing resources. Here are a few helpful hints to safeguard the physical security of items that are your responsibility:

- Never allow another person to use your computer account
- Log out when you leave your computer for long periods of time and “lock” your computer every time you step away
- Close and lock your office door every time you leave
- Use security devices to lock down computers that are in public or otherwise unsecured spaces. Restrict the number of keys to your office
- Know who accesses your office. It may be necessary to maintain an attendance log for high security areas
- Use a screen-saver that requires a password to get back into your computer after the screen saver activates
- Workstation screens should not be visible to anyone but the authorized user of secure documents
- Keep your passwords and computer IDs a secret
- Report suspicious looking persons or activity to the WSU Police department
- Express any concerns about physical security to your supervisor

Security of Surplus Equipment

When university-owned computer systems (desktop/laptop) reach the end of their usefulness in your department, you have the option to surplus that equipment through ESPM (Excess and Surplus Property Management). However, this presents its own share of security risks that need to be addressed. Due to the significant risk of sensitive information leaving the university on hard drives that have not been properly erased, all computers (desktops and laptops) that are being sold through ESPM must have their hard drives removed by CaTS before sending to
ESP. CaTS will ensure proper disposal of the drive. To arrange a removal, contact the CaTS Help Desk at 775-4827.

**Security of Physical Media**
Ensuring the confidentiality of information requires that all physical media (CDs, floppy disks, hard drives, etc) be disposed of properly. This means that, in addition to being properly erased before being discarded, hard drives must also be erased before being returned for any type of warranty work. Additionally, other media such as floppy disks, CDs, DVDs, and paper must also be carefully destroyed if they contain confidential information. Floppy disks should be destroyed by breaking the disk in half, and cutting the center ring with scissors. CDs and DVDs should be broken into multiple pieces, and paper documents should be shredded. If assistance is needed in properly disposing of any physical media, contact the CaTS Help Desk at 775-4827.

**Security of Laptop Computers**
Laptops are easy targets for theft because they are portable. They can be stolen from almost anywhere, including your office. Keeping your laptop secure, especially when traveling, is of utmost importance in order to safeguard university information. Follow the guidelines below to prevent your laptop from being stolen:

- Never leave your laptop unattended in a public place
- During off hours, place your laptop in your office or work area and lock the door
- Place your laptop in a locked drawer or cabinet if you are unable to lock your office or work area
- When traveling, lock your laptop in the trunk of your car, and watch out for potential thieves as you do this
- Do not use your business card as a luggage tag since it discloses your place of work

**Data Theft Techniques**
The rapid expansion and usage of computer technology has brought about many ways for would-be thieves to steal data. In order to help prevent them from doing so, it is helpful to understand some of the data theft techniques that are used. Discussed below are three techniques used most often by thieves.

**Social Engineering**
Social engineering is a term that describes a non-technical kind of intrusion that relies on human interaction and involves tricking people to break normal security procedures. Social engineering relies on the fact the people are unaware of the value of the information they possess and are careless about protecting that information.
Social engineering can occur in many forms:

- A phone call asking for certain information such as a username and password, or other confidential information
- Looking through trash to find printed documents with confidential information about students, faculty, and staff
- A phone call or visit from someone pretending to be an outside consultant or internal system support personnel
- Emails asking for personal information

If you receive a phone call or visit from someone asking you for personal or confidential information, ask questions. Here are a few to ask that may help you stop a potential intruder:

- Ask for their name and correct spelling
- Ask for identification to verify who they are
- Ask for their phone number so you can return their call
- Ask why they need the information
- Ask who authorized the request and let the person know that you will need to verify this information with that authority, and do so immediately

**Phishing**

Phishing is a new type of social engineering used to gather personal information about someone. Phishing refers to email messages that are sent to fool the recipient into providing personal or financial information. These messages are often disguised as an email from a financial institution, such as a credit card company, bank, or e-commerce sites such as eBay and PayPal.

The recipient will receive an "official looking email" asking them to verify account information in order to update their account profile. The email will then ask the recipient to click on an email address or website link, which will take them to the "official" website of that company. The website then asks the recipient to enter personal information. What's not known by the recipient is that this is not a legitimate page, and, by entering personal information into the website, the creators of the website have stolen the information.
If you receive a phishing email, simply delete it. Do not click the links or fill in personal information. Remember, financial institutions will never ask for your personal or account information via email. They have this information already in their records. If you have any doubts or questions about a particular email, contact the organization or company listed in the email to verify the message's authenticity.

**Infected Websites**
Another type of data theft technique is the use of infected websites to obtain a user's personal information. The greatest number of computer infections (nearly 70%) is now coming from exploits that are embedded in websites. These infected websites are most often delivered through email links where a user clicks on the link, and a window opens directly to the website. Once the website is open, a script on the site automatically installs unwanted software on the user's computer without interaction from the user. Often this happens in the background and the user doesn't know about the software. The end result is that the installed software tracks the user's web usage and can collect information such as bank account and credit card numbers, addresses, and Social Security Numbers. These types of infections are similar to phishing, except that these websites do not require user interaction, whereas phishing does. To prevent this type of attack, do not click on links from unsolicited emails or from sources you don’t trust.

**Email**
Email has become one of the quickest and most efficient ways to contact individuals and groups of people. However, using email presents its own set of security risks and challenges that you need to be aware of. Viruses, worms, and spyware are often spread as attachments through email. Here are a few tips to guide you down the path of using email appropriately and avoiding security pitfalls:

- Keep in mind that email is not secure; it can be forged very easily. Never put sensitive information, such as Social Security Numbers or bank account numbers into any part of your email or email attachments
- Faculty and staff: please note that any attachments containing ePI (electronic personal information) must be encrypted before being sent via email
- Do not open unexpected attachments, and do not open or download attachments from unknown parties
- Do not provide tests or assignment grades, evaluations, or final grades via email
- Do not open messages from parties you don't recognize; delete them immediately
- Clear your email inbox of old messages on a regular basis
- Password protect your local email folder file, such as Outlook’s Personal Folder
- Make it a habit not to send any information via email that you wouldn't want disclosed to a third party
- Be careful when forwarding email to others, as many of the emails you receive as forwards are actually hoaxes and may contain viruses
Spam
Spam is unsolicited email. It is a form of advertisement that is sent in mass quantities to email addresses. There's not much that can be done to stop spammers from creating and sending out these messages. The best that we can do is create filters that will block most spam. Spammers are constantly working to find ways around spam filters, so even if filters are turned on and set to their highest setting, some spam email can still get through. If you receive any spam messages, simply delete the email. There are a few things that you can do to minimize the amount of spam you receive:

- Modify your settings on the WSU anti-spam service. You can read more about the service, including how to set it up, by going to http://www.wright.edu/cats/antispam
- Do not click the "unsubscribe" or "remove" link within spam messages; this simply confirms to the spammer that your email address is valid
- Do not give your email address to a person or online website or newsletter without knowing how it will be used. It could end up on a marketing list that is sold to spammers

Protecting Data Integrity
Protecting the integrity of data is another very important step in the overall health of the university’s information. You can do this in a number of ways, most notably through using data encryption methods, backing up the data on a regular basis, and using Virtual Private Network (VPN) software when connecting to university information from home.

Encryption
Encryption is the process of transforming information from clear or plain text into a non-readable format so that only the intended reader can understand or change the message content. Encryption ensures privacy. It is a way to keep prying eyes from reading confidential information that is sent across the public internet.

Certain software applications have encryption methods embedded in them for sending and receiving secure information and for the storage of information. There is also third party software available that can be used to encrypt information.

For directions on encrypting files, check out the “Encryption” area on the following website: http://www.wright.edu/security/itwright/habits.html#integrity

VPN (Virtual Private Network)
A virtual private network (VPN) is a secure and private connection between two points across a public network such as the Internet. A VPN allows users to access their organization's network securely from their homes, hotels, or off-campus public locations.
Any student, staff, or faculty member may use Wright State’s VPN service. You must fill out a form located at [http://www.wright.edu/cats/vpn/](http://www.wright.edu/cats/vpn/) and follow the directions. Contact the CaTS Help Desk at (937) 775-4827 for more information on WSU's VPN service.

**Backups**
One of the most important steps you can take to ensure that the integrity of your data is protected is to backup your files on a regular basis. Data loss can come at any time and for a number of reasons:

- Theft of computer
- File corruption
- Hard drive failure
- Accidental deletion of a file or files
- Viruses
- Natural disasters

You should perform a backup of your files at least once a week, and backup critical files more often if they change. If you need assistance in backing up your files, contact the CaTS Help Desk at (937) 775-4827 and they will be glad to assist you.

**Mobile and Cellular Devices**
Information stored on laptop computers, personal organizers (e.g., Blackberry, Palms), cellular phones, thumb drives, and other similar mobile devices is susceptible to equipment failure, damage, or theft. Information transmitted via wireless connections is not always secure—even networks using encryption are vulnerable to intruders. Below are some tips for protecting information stored on mobile devices:

- Protect and secure mobile devices from theft at all times
- Use internal firewalls and strong authentication when transmitting information via wireless technologies
- Use personal firewalls on laptops that will access the WSU Network from a remote location
- Backup the data on your mobile devices on a regular basis
- Password protect mobile devices when not in use
- Encrypt documents containing sensitive information before they are placed on portable devices
- Charge batteries on mobile devices as soon as the "low battery" prompt appears to avoid losing information, configurations, and settings
# IT SECURITY LINKS

**Wright State University Information Security:**

<table>
<thead>
<tr>
<th>IT Security</th>
<th><a href="http://www.wright.edu/security">www.wright.edu/security</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Do IT Wright</td>
<td><a href="http://www.wright.edu/security/itwright">www.wright.edu/security/itwright</a></td>
</tr>
</tbody>
</table>

**Security Information:**

<table>
<thead>
<tr>
<th>Institute</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Institute</td>
<td><a href="http://www.sans.org">www.sans.org</a></td>
</tr>
<tr>
<td>SANS Storm Center</td>
<td>isc.sans.org</td>
</tr>
<tr>
<td>CERT Coordination Center</td>
<td><a href="http://www.cert.org">www.cert.org</a></td>
</tr>
<tr>
<td>Microsoft Security</td>
<td><a href="http://www.microsoft.com/security">www.microsoft.com/security</a></td>
</tr>
</tbody>
</table>

**Anti-Virus Information:**

<table>
<thead>
<tr>
<th>Information</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Virus Info</td>
<td><a href="http://www.sarc.com">www.sarc.com</a></td>
</tr>
<tr>
<td>McAfee Virus Info</td>
<td><a href="http://www.mcafee.com">www.mcafee.com</a></td>
</tr>
<tr>
<td>Trend Micro Virus</td>
<td>housecall.trendmicro.com</td>
</tr>
<tr>
<td>CERT Virus Center</td>
<td><a href="http://www.cert.org/other_sources/viruses.html">www.cert.org/other_sources/viruses.html</a></td>
</tr>
</tbody>
</table>

**Firewall Information:**

<table>
<thead>
<tr>
<th>Firewall</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone Alarm</td>
<td><a href="http://www.zonelabs.com">www.zonelabs.com</a></td>
</tr>
<tr>
<td>McAfee Desktop Firewall</td>
<td><a href="http://www.mcafee.com">www.mcafee.com</a></td>
</tr>
<tr>
<td>Norton Personal Firewall</td>
<td><a href="http://www.symantec.com">www.symantec.com</a></td>
</tr>
</tbody>
</table>

**Spyware Removal Information:**

<table>
<thead>
<tr>
<th>Spyware Removal</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad Aware</td>
<td><a href="http://www.lavasoftusa.com">www.lavasoftusa.com</a></td>
</tr>
<tr>
<td>Windows Defender</td>
<td><a href="http://www.microsoft.com/athome/security/spyware">www.microsoft.com/athome/security/spyware</a></td>
</tr>
</tbody>
</table>

**Informational Sites:**

<table>
<thead>
<tr>
<th>Information</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snopes (email hoax info)</td>
<td><a href="http://www.snopes.com">www.snopes.com</a></td>
</tr>
<tr>
<td>Phishing</td>
<td><a href="http://www.phishinginfo.org">www.phishinginfo.org</a></td>
</tr>
<tr>
<td>Identity Theft</td>
<td><a href="http://www.consumer.gov/idtheft">www.consumer.gov/idtheft</a></td>
</tr>
<tr>
<td>Internet Fraud Schemes</td>
<td><a href="http://www.lookstoogoodtobetrue.com">www.lookstoogoodtobetrue.com</a></td>
</tr>
</tbody>
</table>
GETTING HELP

For questions, comments, or suggestions concerning this handbook, please contact the CaTS Help Desk using the information listed below. You can also contact the Help Desk for detailed directions on how to accomplish any of the tips, tactics, or directions mentioned in this guide.

CaTS Help Desk
025 Library Annex
937.775.4827
1.888.775.4827
helpdesk@wright.edu