Sensitive Data Security Primer

Only You Can Prevent Security Incidents

Keith R. Watson
CoC Information Security Manager

Abstract

Everyone at Georgia Tech comes in contact with sensitive data every day. The goal of this primer is to provide you with rules of thumb that you can use to recognize and protect sensitive data from unauthorized use and disclosure. Rules of thumb are general guidelines, so this primer will also provide links to more detailed policies and procedures for the classification and protection of sensitive data. This document DOES NOT cover the use or protection of military classified data.

Sensitive Data Security Primer

There are four classifications of sensitive data in use on the Georgia Tech Campus. They are defined in the Georgia Tech Data Access Policy.

http://www.oit.gatech.edu/sites/default/files/DAP.pdf

The data classifications are:

Category I - Public Use: This information is targeted for general public use. Examples include Internet web site contents for general viewing and press releases.

Category II -Internal Use: Information not generally available to parties outside the Georgia Tech community, such as directory listings, minutes from non-confidential meetings, and internal (Intranet) web sites. Public disclosure of this information would cause minimal trouble or embarrassment to the Institute. This category is the default data classification category.

Category III - Sensitive: This information is considered private and must be guarded from disclosure; unauthorized exposure of this information could contribute to ID theft, financial fraud and/or violate State and/or Federal laws.

Category IV - Highly Sensitive: Data which must to be protected with the highest levels of security, as prescribed in contractual and/or legal specifications.

There are 16 simple rules of thumb that can be used to guide you in recognizing and protecting sensitive data.

Rule of Thumb 1- When in doubt always assume data is sensitive until proven other wise.

Rule of Thumb 2 - When in doubt don't give it out.

Rule of Thumb 3 - Only save sensitive data in approved locations.

Rule of Thumb 4 - Never save credit card numbers.

Rule of Thumb 5 - Printed and handwritten material must not contain credit card numbers.

Rule of Thumb 6 - Never publish anything on a web page you wouldn't want your mother to read on the front page of the Atlanta Journal-Constitution.

Rule of Thumb 7 - Always securely delete sensitive data that is accidently saved to an unapproved location.

Rule of Thumb 8 - Never send sensitive data in email.

Rule of Thumb 9 - Never store sensitive data on a laptop without encryption.

Rule of Thumb 10 - More data about a student than is published in the campus directory should be considered sensitive.

Rule of Thumb 11 - More data about a member of the faculty or staff than is published in the campus directory should be considered sensitive.

Rule of Thumb 12 - Always retain data (sensitive or other wise) for the least amount of time possible.

Rule of Thumb 13 - When in doubt, shred printed documents using a crosscut shredder.

Rule of Thumb 14 - When in doubt, always shred recorded media.

Rule of Thumb 15 - Never give your password to anyone.

Rule of Thumb 16 -Always use a strong password.

Rule of Thumb 1 - When in doubt always assume data is sensitive until proven other wise.

If you have questions about the sensitivity of data you come into contact with, assume that it is sensitive; then ask for help in determining its classification. A very helpful resource in determining the classification of sensitive data is the Georgia Tech Data security Classification Handbook.

http://www.oit.gatech.edu/sites/default/files/DSC_handbook.pdf

Here are some rules of thumb for identifying sensitive data:

- List of Names with Birthdays
- List of Employee Names and Home Addresses
- Travel reimbursement forms
- Financial data
- HR data
- Personal information that can be used for identity fraud (see Rule of Thumb 9 for more detail)
- Social security numbers
- Credit card numbers
- Any student data that is not listed in the campus directory (see Rule of Thumb 8 for more detail)
- Research project data

If you need help in determining the classification of data you can contact the CoC Information Security Manager.

Keith Watson
krwatson@cc.gatech.edu
404-385-7401

Rule of Thumb 2 - When in doubt don't give it out.

If you are asked to give someone sensitive data and you are not sure if they are authorized to have it then don't give it to them until you are sure it is OK. Also never honor Freedom of Information Act and Georgia Open Records Act requests without consulting the Georgia Tech Office of Legal Affairs.

Georgia Tech Office of Legal Affairs Open Records Act Procedures
http://www.legalaffairs.gatech.edu/topics.html#anchor378715

This rule of thumb is one of the harder ones to use. By our nature we all want to help people when they are in need and we want to be liked. Social Engineering is the art of taking advantage of our nature to gain unauthorized access to sensitive information. We must be ever vigilant. This is especially true of student information.

It's moderately difficult to buck our nature and deny access over the phone or in email but it is exceptionally difficult to do it in person. This is a problem for the Social Engineer. He will get better results in person but this puts him at risk of being caught and detained by the astute employee. Asking for unauthorized access over the phone or in an email is less risky but it doesn't get as good a result. You must always be on your guard when asked to provide sensitive data to someone outside of your normal work process.

Rule of Thumb 3 - Only save sensitive data in approved locations.

Always save sensitive data on the Adminfs server in a directory approved by your manager. Contact the Information Security Manager if your department needs help setting up a secure directory.

Never publish sensitive data on a web page or save sensitive data on your H: or S: drives, desktop computer, laptop computer, or removable media such as a floppy disk, CD, DVD, or USB key. When in doubt ask. This rule cannot be stressed enough.

Several of the most recent security incidents would have been prevented if sensitive data had not been stored in an insecure location. There are exceptions to this rule but they have to be authorized in advance and special precautions have to be put in place. The Georgia Tech policies and procedures that address the operation of systems that store sensitive date can be found here:

Computer & Network Security Procedures
http://www.oit.gatech.edu/sites/default/files/CNUSP.pdf

Georgia Tech Credit Card Processing Procedures
http://www.oit.gatech.edu/georgia-institue-technology-credit-card-processing-procedures

Data Protection Safeguards
http://www.oit.gatech.edu/sites/default/files/GIT_Data_Protection_Safeguards.pdf

Safeguarding Information on Laptop Computers
http://www.oit.gatech.edu/security-travel-tips-laptops

Rule of Thumb 4 - Never save credit card numbers.

Never save any documents in electronic form that contain credit card numbers on any computer or media. CoC does not operate any computer systems or storage devices qualified to store credit card numbers. These are the policies and procedures regarding credit card data:

Georgia Tech Credit Card Processing Policy
http://www.oit.gatech.edu/sites/default/files/Credit_Card_Processing_Policy.pdf

Georgia Tech Credit Card Processing Procedures
http://www.oit.gatech.edu/georgia-institue-technology-credit-card-processing-procedures

Data Protection Safeguards
http://www.oit.gatech.edu/sites/default/files/GIT_Data_Protection_Safeguards.pdf

Georgia Tech Data security Classification Handbook.
http://www.oit.gatech.edu/sites/default/files/DSC_handbook.pdf

Rule of Thumb 5 - Printed and handwritten material must not contain credit card numbers.

Printed and handwritten material must not contain credit card numbers. In cases where a credit card number is required, all digits but the last four must be blacked out. This includes but is not limited to credit card receipts and travel reimbursement forms,

Georgia Tech Data security Classification Handbook.
http://www.oit.gatech.edu/sites/default/files/DSC_handbook.pdf

Georgia Tech Credit Card Processing Policy
http://www.oit.gatech.edu/sites/default/files/Credit_Card_Processing_Policy.pdf

Georgia Tech Credit Card Processing Procedures
http://www.oit.gatech.edu/georgia-institue-technology-credit-card-processing-procedures

Rule of Thumb 6 - Never publish anything on a web page you wouldn't want your mother to read on the front page of the Atlanta Journal-Constitution.

You may be very careful to never publish sensitive data on a web page but you may be divulging information that should not be shared with a complete stranger. Remember that once you publish information on a web page it can never be completely removed. You may delete your web page but copies are kept for all eternity at sites such as google.com and archive.org. The Georgia Tech World Wide Web Publishing Guidelines can be found here:

http://www.oit.gatech.edu/guidelines-concerning-publication-information-world-wide-web

Rule of Thumb 7 - Always securely delete sensitive data that is accidently saved to an unapproved location.

There are tools for securely deleting sensitive data from an insecure location. Contact the CoC Information Security Manager if you do not have these tools or do not know how to use them. Most of the commonly used tools for securely deleting data do not work on USB keys. A special process must be used. When in doubt ask for help. There is no shame in reporting improperly saved sensitive data before it leads to a security incident.

Rule of Thumb 8 - Never send sensitive data in email.

Email is not secure and like web pages you cannot control where emails end up going or what system they might be stored on. For example, an email is sent to a faculty email list that contains sensitive student data. Members of the email list may have their email forwarded to non-Georgia Tech systems. These systems are not secure. They may read their email on a laptop or cell phone. Is the laptop or cell phone secure? What if it is stolen during a business trip? Did you like it when you received a letter saying your sensitive data has been compromised because a laptop was stolen? I know I didn't like it when it happened to me.

I realize this rule of thumb is very controversial as email is commonly used for all manner of business communication. As such, it has become the default method to quickly communicate with a large number of people. Sometimes it isn't possible to avoid using email. Georgia Tech currently doesn't have an email policy; however, one is being written.

In the interim here are some suggestions on how to send information via email without divulging sensitive information.

1. Save the information on a secure server and then provide the location of the document in the email. This will avoid sending sensitive data in the email itself and only authorized users will be able to access the data on the server.

2. Encrypt the email. This is a bit more problematic as most people have never used email encryption and most recipients are not prepared to receive it.

3. If you must use email containing sensitive data as part of a business process then the process should be reviewed with your manager and the CoC Information Security Manager to insure there is no other way of sending the data in a secure manner.

Rule of Thumb 9 - Never store sensitive data on a laptop without encryption.

Laptops are often taken for granted. We use them to read email, to telecommute, and as desktop replacements. It is very easy to forget that laptops are one of the most common sources for unauthorized disclosure of sensitive information. As a result laptops deserve a rule of thumb all their own despite previously being discussed in rules of thumb 3 and 4. Laptops are also growing concern for government and business travelers as they are common targets for government sponsored and corporate espionage.

The grave concern over laptop security has led to the recommendation that sensitive data is never to be stored on a laptop. If you have any questions regarding your laptop's security, please contact the CoC Information Security Manager. If you have a laptop, you must comply with the Georgia Tech Guideline Safeguarding Information on Laptop Computers.

http://www.oit.gatech.edu/security-travel-tips-laptops

If you are traveling, I also recommend the IBM Security Systems Cyberspying guidelines by Gunter Ollmann.

http://blogs.iss.net/archive/cyberspying.html

Rule of Thumb 10 - More data about a student than is published in the campus directory should be considered sensitive.

The campus directory provides a web-based way of looking up contact information for Georgia Tech faculty, staff, and students.

http://www.gatech.edu/directories/

The Family Educational Rights and Privacy Act (FERPA) allows a student to request that Georgia Tech restrict access to any of their data without a written release from the student (the confidential indicator). When the confidential indicator is set, Georgia Tech is not permitted to give ANY of the students data to anyone including their parents without written permission from the student. Refer to the Confidentiality and Request No Print web page on the Georgia Tech Registrar's web site for more detailed information about this issue.

http://www.registrar.gatech.edu/students/formlanding/confid.php

Another excellent resource is the Georgia Tech Student Directory Information Disclosure DOs and DON'Ts.:

http://www.datacleanup.gatech.edu/pdf_docs/Disclosing_Student_Info_Guidelines.pdf

So how can you tell if a student has set the confidential indicator? If the student doesn't show up in the campus online directory you must assume that the confidential indicator has been set.

Rule of Thumb 11 - More data about a member of the faculty or staff than is published in the campus directory should be considered sensitive.

The campus directory provides a web-based way of looking up contact information for Georgia Tech faculty, staff, and students.

http://www.gatech.edu/directories/

You should be very careful not to divulge any more information about faculty or staff than is published in the online directory as it can be used for Social Engineering at the least and identity theft at the worst. When in doubt ask your manager or the CoC Information Security Manager.

Rule of Thumb 12 - Always retain data (sensitive or other wise) for the least amount of time possible.

Due to the risk of leaking sensitive data and the increasing legal risks of electronic data discovery (this includes Freedom of Information Act and Georgia Open Records Act requests) it is recommended that you retain data for the least amount of time possible. These are the policies and procedures concerning data retention:

Board of Regents Retention Guidelines
http://www.usg.edu/usgweb/busserv/series/index.phtml

Georgia Tech Data Protection Safeguards
http://www.oit.gatech.edu/sites/default/files/GIT_Data_Protection_Safeguards.pdf

Georgia Tech has an annual Data Cleanup Campaign to promote locating sensitive data in electronic or printed form and insuring it is stored correctly. The campaign also promotes expiring data that is no longer needed. The Georgia Tech Data Cleanup Campaign web site covers this in more detail.

http://www.datacleanup.gatech.edu/

Rule of Thumb 13 - When in doubt, shred printed documents using a crosscut shredder.

When you are disposing of printed documents and you have any doubts as to whether they contain sensitive data you should shred the documents with an approved shredder. The type of shredder used depends on the sensitivity of the data, but the best rule of thumb is to always use a crosscut shredder. The CoC Information Security Manager can provide you with a shredder recommendation if you need one for you or your department.

Georgia Tech has a contract with a secured shredding service for those times when you have a large quantity of material to shred (large being more than you are willing to do with your departmental or personal shredder). Contact the CoC Information Security Manager to arrange for this service.

Rule of Thumb 14 - When in doubt, always shred recorded media.

When you are disposing of any form of recorded media such as but not limited to CDs, DVD's, USB keys, floppy disks, hard drives, and backup tapes, they must be shredded. Never just throw it in the trash. The data on the media may be recoverable even when the data has been deleted.

Georgia Tech has a contract with a secure media destruction service. They can securely destroy any type of recorded media.

If you have recorded media, such as a hard drive, that contains sensitive data and you need to reuse it for non-sensitive data the CoC Information Security Manager can help you securely wipe the media so it can be reused. A common example of this is when a staff member gets a new computer and their old one is given to another user. Before the machine is redeployed, the hard drive can be securely wiped so the new owner is not exposed to sensitive data.

Rule of Thumb 15 - Never give your password to anyone.

Never give your password to anyone. Section 3.1.7.1 of the Georgia Tech Computer & Network Usage and Security Policy (CNUSP) explicitly prohibits sharing your password with anyone, including your manager.

http://www.oit.gatech.edu/sites/default/files/CNUSP.pdf

If there is an emergency while you're out of the office your data can be accessed via an approved procedure. If this occurs, contact the CoC Information Security Manager for assistance.

Rule of Thumb 16 -Always use a strong password.

You can be diligent in every aspect of handling sensitive data but the “bad guys” can guess, or use a computer to break, a weak password, and then they can access the data as if it were you.

Your password should contain a minimum of 8 characters from all of the following character classes:

- Uppercase letters
- Lowercase letters
- Numbers
- Punctuation

Here’s an example of how to pick a good password:

Pick an easy to remember phrase

Four score and seven years ago our forefathers

Take the first letter of each word

Fsasyaof

To create a good password that is easily remembered, substitute characters that sound the same, have the same meaning, or begin with the same letter (example: 3 begins with the letter T)

4S&7y@Of

Don’t use the example above as your password.

How to pick a good password DOs:

- Do use a password of at least 8 characters
- Do use upper and lower case letters, numbers, and punctuation
- Do use an acronym from an uncommon phrase
- Do use homonyms for letters.
- Do change your password every 90 days.
- Do use a password "wallet" for infrequently used passwords

How to pick a good password DONTs:

- Don't use any word that can be found in an English or foreign dictionary
- Don't use abbreviations of common phrases or acronyms, e.g., asits9 (a stitch in time saves nine), wysiwyg (what you see is what you get), or tanstaafl (there ain't no such thing as a free lunch).
- Don't use common literary names such as Baggins, Popeye, etc.

- Don't use any password containing your login ID spelled backwards.
- Don't use any password containing one of your names or initials, or any combinations thereof
- Don't use any password involving personal data, such as your address, maiden name, relatives' names (e.g., spouse's and children's first names), pets' names, hobbies, favorite sports teams, etc.
- Don't use any password consisting of sequences such as "abcdef"
- Don't use any password consisting of consecutive keys such as "qwerty"
- Don't use any password consisting of repeated sequences
- Don't use any password given to you when your account was set up
- Don't reuse old passwords

Additional Resources:

Georgia Tech Security Policies, Standards, and Procedures
http://www.oit.gatech.edu/service/information-security/security-policies-standards-and-procedures

Georgia Tech Computer & Network Usage and Security Policy (CNUSP)
http://www.oit.gatech.edu/sites/default/files/CNUSP.pdf

Georgia Tech Security Awareness Tutorial
http://www.security.gatech.edu/information/safe/

CoC Information Security Manager
Keith R. Watson
krwatson@cc.gatech.edu
(404) 385-7401

TSO Help Desk
Walkup M-F 7:00 A.M. to5:00 P.M.
helpdesk@cc.gatech.edu
AIM - TSOHlpDsk
(404) 894-7065