

MSA Practicum

Computer and Data Security

Policy and Guidelines

Definitions

Backup Drive – A network drive connected to the Practicum Server that is dedicated for backup content.

Head of Data Security (HDS) – The IAA staff member in charge of security and architecture for the Practicum computing environment, as well as being responsible for data transfer with the Sponsor. The HDS is also in charge of securely erasing data and documenting processes.

IAA (Suite)– The 1st and/or 2nd floors of the Alliance 1 building containing the Institute for Advanced Analytics.

Sponsor – The company supplying the problem statement and the data sets to the Practicum Team.

Data Transfer Portal – A secure, encrypted web site (portal, e.g. <https://send.iaa.ncsu.edu>) for sending and receiving Data and sensitive communications to the Sponsor.

Data, Sponsor Data, Practicum Data – Confidential information shared by the Sponsor under a non-disclosure agreement, including work and materials created by the Practicum Team (in any form e.g. paper and electronic documents) in relation to the Practicum. This includes code written by students, data generated by such code, presentation and organizational materials.

NDA – Non-Disclosure Agreement. A legal document issued by the Sponsor describing the terms of use, and protection, of the Data.

Practicum Server – A dedicated computer for the Practicum Team located at the Institute for Advanced Analytics.

Practicum Team – The 4, 5, or 6 person team assigned to a Sponsor project.

Prohibited Data / Personally-Identifiable Information (PII) – Data containing personally-identifiable or financially-sensitive data. This can include Social Security numbers, full names, addresses, phone numbers, account numbers, among other identifying fields. It is not allowed, except in special circumstances such as already being publically available, or not referencing an individual person (e.g. business address).

Student Laptop – The laptop used by the student on a daily basis. The Student Laptop is used to access the Practicum Server.

Tech Lead – The person from the Practicum Team designated to be the primary contact point with the Head of Data Security.

1.) Policy Statement

—The objective of these policies and guidelines is to ensure that Practicum data is protected in all of its forms, on all media, during all phases of its life cycle (generation, use, storage and disposal) from unauthorized or inappropriate access, use, modification, disclosure, or destruction. This policy applies to all Sponsor Data and documents received by the Institute and its students regardless of additional non-disclosure agreements (NDAs) or their absence.

2.) Policy Compliance

—Violations of the “MSA Practicum Computer and Data Security Policy and Guidelines” will result in a verbal warning, with repeat violations resulting in serious consequences or possible termination from the MSA Program.

3.) Responsibilities

—Students are individually responsible for full compliance with these policies and guidelines and will sign the Practicum Computer and Data Security Agreement form (electronically) in addition to any non-disclosure agreement (NDA) as required by the Sponsor.

—Students will only use the sponsored Practicum Data and Practicum Server for purposes appropriate to the goals and objectives of their Practicum. (Do not use them for homework or side projects.)

—The Institute for Advanced Analytics (IAA) will likewise take all precautions stated in this policy to keep Data secure.

—Sponsors are instructed to not include personally-identifiable or financially sensitive data when transmitting data sets to the Institute or its students. Students will verify this, because PII is found **every year!** (See Section 5)

—The Head of Data Security will ensure secure disposal of Data at the end of the project that resides on university-owned equipment. The HDS will document this secure erasure.

—The Student will ensure secure disposal of any Data that resides on personally-owned equipment (e.g. shredding paper notes.) The HDS will document this secure erasure.

4.) Interacting with IAA IT

—The Practicum Team will designate a “Tech Lead” who will be the primary contact point with the IAA IT Team. This person does not need to be technically savvy, although that would help. There will be occasional communications among the Tech Leads to report and disseminate information that Practicum Team members will need to know (tips and methods for working with software and Data). The Tech Lead will be responsible for conveying this information to the rest of the Practicum Team.

Additionally, it is preferable that the Tech Lead brings requests to the IAA IT Team rather than requests coming from individual Practicum Team members. If the Tech Lead is unavailable to do this at a particular time, other Practicum Team members may interact directly with the IAA IT Team.

5.) Data Transmission / Interacting with Sponsors

5a.) Only Use Acceptable Data Transfer Methods

—Sponsored Practicum Data will be transmitted in a manner that is secure and acceptable to both the IAA and the Sponsor. Do not get creative about Data transfer. Likewise, do not let the Sponsor get creative about Data transfer (e.g. don't let them email you file attachments or download links.)

5b.) Data Transfer Portal

—In most cases, data transfer will utilize a secure web application (also known as: the Data Transfer Portal) dedicated for the Practicum: <https://send.iaa.ncsu.edu>. Both the Sponsor and the Practicum Team can log in, send, and receive data to each other utilizing strong encryption. The HDS may inform a Practicum Team of approved exceptions to this method. If the Sponsor informs the Practicum Team of a secure alternative data transfer method, ensure that the HDS is aware of this immediately.

5c.) Email / Google Drive Banned on Practicum Server

—The Practicum Server does not allow web access to GMail, Google Drive, nor similar cloud-based data transfer services. Students can use their laptops to correspond above the NDA to the Sponsor via GMail, but not for transferring any Data (nor sensitive communication). Exceptions may be granted by the HDS for special circumstances. Do not allow Sponsor to email you sensitive Data or attachments (e.g. data dictionaries).

5d.) Example of Practicum Team / Sponsor Communication Involving Practicum Data

—If the Practicum Team needs to ask detailed questions of the Sponsor, and perhaps send code or Data snippets, the preferred method is to upload a Microsoft Word / Excel / PowerPoint document to the Data Transfer Portal. The Sponsor will upload a response document similarly. This way, email (which is not secure!) will be avoided for sending sensitive communications or NDA content/data. Email is only acceptable for high-level communications not under the NDA (such as coordination.) Suggested use: email the Sponsor from your laptop that you have some detailed questions (or deliverables) waiting in a document on the Data Transfer Portal, and request that they send responses (or deliverables) through the Data Transfer Portal in return. Talk to the HDS if Data Transfer Portal is not used by your sponsor.

5e.) *Never Transmit Data or Passwords Insecurely*

—Data (including NDA-sensitive written communications, or code) and/or passwords shall **NEVER** be transmitted in raw, unencrypted form over an insecure medium (such as email / Slack / text message). I.e. no emailing/Slack-messaging of unencrypted Excel spreadsheets, code snippets, etc., is allowed. No emailing/Slack-messaging/text-messaging of passwords is ever allowed! The IAA-provided messaging platform, Mattermost (e.g. <https://prac#-mattermost.iaa.ncsu.edu>), is a secured medium hosted at the IAA for this purpose and therefore an exception to this guideline.

5f.) *Some Clarification of Data Transfer Methods*

Method	Acceptable?
Log in to secure Data Transfer Portal to send or receive data to the Practicum Server (https://send.iaa.ncsu.edu)	Yes. Sponsor may choose alternate secure method (HDS would notify you of this.)
Send decryption password over (voice) telephone e.g. to Sponsor	Yes.
Emailing/Slack-messaging decryption passwords, Data, code	No!
Using IAA's secure Mattermost service to share passwords, Data, code internally within Practicum team	Yes, though unlikely to be necessary.
Uploading Data / code to Google Drive (either for you, or to share)	No!
Encrypting Word / Excel / Powerpoint with strong password, and then emailing attachment to Sponsor	Not allowed by policy, although adequately secure. Email not accessible on Practicum server. Ask HDS for advice here.
Encrypting a .zip / .7z archive with a strong password, and then emailing to Sponsor	Not allowed by policy, although adequately secure. Email not accessible on Practicum server. Ask HDS for advice here.

Encrypt USB drive with Microsoft BitLocker with a strong password, and copy Data or presentation materials onto it to carry to Sponsor headquarters.	Only with assistance from HDS. Common activity during final presentations if off-site travel is required. IAA provides the USB drives and facilitates insertion/retrieval of USB drives to server.
--	---

5g.) *Encryption Passwords*

—Encryption passwords must be strong passwords (see Appendix A, although IAA IT Team creates these for you) Ability to defeat encryption is proportional to simplicity and shortness of encryption password.

It is unlikely you will need to create strong passwords yourself, but you should understand this information. Never email / text-message / Slack-message passwords because the information can be intercepted by others!

5h.) *Prohibited Data / PII*

—When you receive Data through an approved, secure method, ensure no Prohibited Data is present.

Prohibited Data is defined as *personally identifiable information* (PII) or *sensitive financial information*. Some examples of Prohibited Data are:

• Social Security Numbers	• Personal phone numbers	• Full personal addresses
• Full names	• Credit card numbers	• Bank account numbers

The Practicum Team will determine how much effort and what procedures are necessary to comfortably make the assurance that the Data is clean of Prohibited Data. Software is provided to assist with this task. An electronic (Google) form to demonstrate assurance will be provided by the Head of Data Security to be filled out EACH time new Data is transferred to the Practicum Team (potentially many times before graduation).

If violations occur, the entire Data transfer must either be securely erased by the HDS and the cleaned Data retransmitted by the Sponsor, or in certain circumstances the HDS may allow the tainted data itself to be extracted.

Violations of personally-identifiable information are detected by Practicum Teams every year. In the 2013-2014 academic year, 31% of data transfers from Sponsors had concerns or violations. Please do not undervalue this exercise.

5i.) *Online Meetings*

—Online web conferences (e.g. Zoom, WebEx, Google Meet) are acceptable and encouraged, as long as certain criteria are followed:

a.) **Do NOT record meeting video yourselves. Do NOT hit the Record button in Zoom.** It is not acceptable *for the practicum team* to record meeting video, because it will send sensitive Practicum discussion (covered by the NDA) to either cloud services for processing, or your laptop (which is not allowed to have sensitive NDA content). *If the sponsor hosts the meeting on their platform*, then *they* can record the meeting for themselves and upload it to the Data Transfer Portal for the team to access on the Practicum Server.

b.) Recording meeting audio is technically possible, though not encouraged, but only if using a specific method authorized by the HDS. Inquire with the HDS for instructions for the authorized audio recording method.

Ensure unauthorized guests cannot access the meeting. Either use Zoom's Waiting Room, or if no other choice is available, meeting passwords. If the web conference automatically emails meeting passwords, then that is a rare authorized exception to Section 5e of this document.

6.) Physical Security

Physical security is an important but often under-valued topic. If you leave your laptop open in a coffee shop and go to the restroom and it gets stolen, one must assume in the worst-case that the thief has full access to whatever you were doing. Be aware of your surroundings and consider “what could possibly go wrong” as a factor in your decisions.

6a.) Student Laptop

—Do not leave your laptop lying around, whether that is in the IAA classroom, or a bench in the library, or the back seat of your car, or a coffee shop table. There have been multiple thefts from the Venture 2 building (old IAA location) over the years. When at the IAA, use your lockers to store your laptop if you do not carry it with you. In other locations, use good judgment so you do not tempt opportunistic thieves. If you do step away from your laptop, at least lock the screen so that your password is needed to gain access.

6b.) Notebooks, Papers and Other Resources

—Be organized about where you store any written notes, printed pages, or other materials related to your Practicum. Any Practicum materials that reside in hard copy form must be accounted for and securely destroyed at the end of the Practicum. The Head of Data Security will assist and document this secure destruction.

6c.) Whiteboard Usage

—Be sure to adequately erase any whiteboards that you use during Practicum team meetings. If the meeting rooms at the IAA are not adequately stocked with erasing materials (including solvent spray), ask a staff member for assistance. In other settings, assess the erasing methods before you begin writing.

6d.) Visibility In Public Settings

—In public settings, such as the glass-walled meeting rooms at the IAA, Hunt Library, or an open meeting space, the Practicum Team must be cautious and aware of the surroundings. Use mini-blinds for privacy when possible. Do not allow people passing by to be able to view NDA material. Consider how exposed you are, and the kind of content displayed on a display. Certainly do not put presentation slides up where non-team members can see them. Consider the 1st floor meeting rooms with windows to the outside sidewalk...

6e.) *IAA Suite Entrance Policy*

—If an unknown person follows you into the IAA Suite, alert IAA Staff immediately. You are not required to engage the unknown person. If a non-student or non-instructor knocks at the door or rings the doorbell, you should not answer the door. The doorbell is intended to alert IAA Staff who will answer the door. If you see a violation of this policy, you should alert IAA Staff. There are several scenarios where unauthorized persons would attempt to gain access to the IAA Suite, and we must be cautious to detect this unauthorized access. If you let someone in the suite, ask their name and tell a staff member what happened.

7.) **Student Laptop Security and Acceptable Use**



Your laptop is arguably the weakest link in the security chain because it alone has the access (with your credentials) to the Practicum Server. If your laptop is compromised, taken-over, or stolen, emergency measures must be enacted by the Head of Data Security and the Practicum Team.

7a.) *Login Password / PIN*

—You must use a login password, PIN, or fingerprint for your Windows/macOS account.

7b.) *Lock Screen When Not In Use / Prevent Unauthorized Access*

—You must prevent the possibility of someone accessing your Student Laptop without your permission. If you walk away from your laptop, you must lock the screen or do something to require password authentication to regain access (e.g. close the lid, putting the laptop to sleep).

Press the  key and the “L” key (Windows) or -Ctrl-Q (macOS) at the same time to lock the screen when you walk away, or else put the laptop to sleep. Test these methods. Insure they work as intended.

7c.) *Windows/macOS Updates*

—You must keep current on Windows or macOS Updates on your Student Laptop.

At least by the end of each month you should install any Windows or macOS Updates that are available.

7d.) Other Software Updates

- You must keep the following software updated:
 - Web browsers (any that are installed)

7f.) Antivirus Software and Scans

- You must have antivirus software installed on your laptop. You should complete a full manual (or scheduled) scan every month, or more frequently. If virus or malware is detected, you must alert the Head of Data Security because sometimes antivirus software misleads you to believe it has deleted a virus when it has not truly succeeded.

7g.) Illegal Downloads, Warez, Poor Web Browsing Choices, Sharing USB Drives

- Many viruses detected on Student Laptops in the past have been due to downloading software from illegitimate sources, browsing from sketchy websites (which persuade you to download and run applications), or sharing USB drives (although there are many other mundane ways to get viruses). You must be cautious and diligent in conducting safe computer usage. Antivirus software will not always protect you, so you must use good judgment. Be careful when installing software to not accidentally install unnecessary “add-on” software (like web browser toolbars). Keeping your software current (see previous item) is also an important defense.

7h.) Avoid Sharing Your Laptop

- You must be very cautious about sharing access to your Student Laptop to anyone else. Roommates, children, and spouses that use your laptop do not have the same incentive and perspective as you do about security. If you must share your laptop, please use a strong password and grant access to a “Standard” account and not an “Administrator” account (if the user protests at this, this is a red flag). Please avoid this altogether if at all possible.

8.) Message Security – Email / Slack / Text Messaging / etc.

A major way malware infiltrates begins with email. A user clicks a malicious link, a web browser opens, and a malicious website loads. Email is also fundamentally insecure. The “From:” field in an email is trivial to forge, just like on a paper envelope. Forget about the “https” secure protocol in the URL for Gmail, and just assume that email is plaintext, unencrypted, readable-by-all like a post card in the physical world.

8a.) *Emailing Sensitive Practicum Information*

—Files containing NDA data should never be sent or received unencrypted through email. **Do not let the Sponsor send you data like this.** Talk to the Head of Data Security if you desire to send *encrypted* data files between you and the Sponsor through email (**this is RARE**). Violations should be reported to the HDS for proper incident handling. **The Data Transfer Portal (<https://send.iaa.ncsu.edu>) is the preferred secure data transfer method instead of email.**

8b.) *Emailing General Information*

—Emailing *general information 'above the NDA'* between your Practicum Team and Sponsor is acceptable as long as you use good judgment. You should avoid sending documentation through email to your fellow Practicum Team members if it can be shared through e.g. Microsoft OneNote on the Practicum Server (example: output results from an analytical procedure). Reserve email/Slack for coordinating and logistical types of high-level communication.

8c.) *Email Deletion at End of Practicum*

—At the end of the Practicum, you should expect to search your email for all Practicum communications to the Sponsor and delete these messages. The HDS will guide you through this process. Data at rest is a liability, including email communication about Practicum. When the Practicum is over, only the Sponsor should have any remnants of it.

8d.) Email Safety

—Be cautious about clicking any links in emails (i.e. hover over the link and discern its true destination) in emails (even “unsubscribe” links in mailing lists), even if you think you know the sender. The sender of an email can be easily faked, and sometimes friend’s email accounts are hacked. Attackers will try to bait friends and relatives into clicking malicious links based on the automatic trust you have with your friends. Your Student Laptop, or the Practicum Server, can be infiltrated this way. Hover your mouse over a link before clicking to see where it really leads. Be careful.

8e.) Use of Communication Tools Such as Slack, WhatsApp, etc

—Slack is acceptable for high-level communication and logistical coordination, just like email. For detailed discussion of the project, which is low-level (“beneath the NDA”) communication, **you can not use Slack, WhatsApp, etc.**

—NEVER send Data, passwords, or any kind of sensitive content through Slack or a similar communication tool. Assume it is NOT a secure medium by default.

8f.) Use of IAA-Provided Communication Tool: Mattermost

—Similar to Slack, but hosted in-house at the IAA datacenter, Mattermost provides Slack-like messaging capability within the Practicum server’s Remote Desktop environment. At this time it is not possible to use Mattermost from smartphones, so you will log in to the Practicum server and access it through Google Chrome. All Mattermost communications will be securely deleted by the HDS at the end of the academic year.

9.) Google Account Security

9a.) *Verify that your NCSU Google account is not granting unauthorized 3rd-party access.*

- Log in to your NCSU webmail, then go to <https://security.google.com>
- Click “Security Checkup – Get Started”
- You will be guided through the Security Checkup. Click “Learn More” or ask the HDS for help if you have concerns.
- Remove any “account permissions” that are no longer being used or needed. Report suspicious activity to the Head of Data Security.

9b.) *2-factor Authentication for Google Account*

—You are required to use 2-factor authentication (a.k.a. “two-step” or 2FA) with your NCSU Google account.

9c.) *Access To Google Account From Other Computers*

—Be cautious about logging in to your NCSU Google account from another computer, such as a friend or family member’s computer. Just assume that your roommate’s computer is full of viruses or keystroke loggers. If you must, at least be sure to Sign Out when you are finished using websites, and clear web browser history and cookies. If you do not, it is feasible that another person could effortlessly hijack your account if the session is still active. This is common in Internet café’s. (2-factor authentication may not help you!) Assume NCSU computer labs are safe, however, due to unique, authenticated login sessions.

10.) Smartphone Security

For many people, their smartphone (Android, iPhone, etc) is the weakest link in their privacy and security (i.e. the easiest way to hijack a person's email account).

10a.) Password / PIN on Smartphone Home Screen

—Some people do not use a password on the phone, and remain logged in to major email accounts and social media.

If your smartphone is logged in or connected to your NCSU Google account, you must use a password (or PIN, fingerprint, faceID, or similar) on your smartphone to unlock. There are different options available depending on your device. Ensure that there is an appropriate timeout period when the phone will lock itself when not in use.

10b.) Bypassing Smartphone App Store

—Do not download apps outside of approved marketplaces (approved marketplaces are e.g. Google Play, Apple App Store). These marketplaces verify that apps meet certain security requirements and are considered trustworthy (enough). If you have jailbroken your device in order to sideload apps, this could be a problem and may need to be discussed with the HDS.

11.) Practicum Server Access (See Appendix for Log In instructions)

11a.) Remote Desktop Connection

—You must use the official Microsoft Remote Desktop Connection software that comes with Windows (or the official Microsoft version for Mac OS) in order to connect to the Practicum Server unless the Head of Data Security has made a special written exception to you (e.g. Linux users).

11b.) Unattended Laptops

—Do not leave a Remote Desktop session open on your Student Laptop when you are not present. Lock the screen of your Student Laptop, and optionally Log Out or Disconnect from the Remote Desktop session.

12.) Practicum Server Security and Acceptable Use

12a.) Data Ingress/Egress

—Do not transfer Data off of the Practicum Server unless directed to do so by the Head of Data Security (e.g. presenting at Sponsor headquarters on encrypted USB drive). **Do not transfer Data onto your laptop in order to work (i.e. do analytics) with it. Do not let the Sponsor send Data to you via email without permission from the HDS first (it shouldn't happen).** Secure data transfer should occur through the Data Transfer Portal (<https://send.iaa.ncsu.edu>) accessible by both the Practicum Team and the Sponsor.

12b.) Backups of Practicum Server Data

—Backups are to be made only to the “X:\ Backup Drive” attached to the Practicum Server. Do not back up data yourself off of the server; neither to Google Drive, nor to OneDrive, nor to your laptop.

12c.) No Data on Laptops

—**You should never have unencrypted Data on your Student Laptop.** Alert the Head of Data Security if violations occur so the data can be securely erased and documented. The HDS may grant permission to carry encrypted Data (e.g. for a Sponsor presentation on-site) but the HDS will facilitate the creation/encryption of this USB drive.

12d.) No Data in the Cloud (i.e. outside the IAA datacenter)

—You should never have Data (reports, code, raw data) in any “cloud services”, which means Data leaves the IAA datacenter and is accessible by employees of the cloud service. Examples include ChatGPT, Grammarly, Slack, Dropbox, Google Drive, One Drive, Tableau Public Server, Anaconda Cloud, GitHub.com, etc. IAA-provided services such as Gitlab (e.g. `prac#-git.iaa.ncsu.edu`) or Mattermost (e.g. `prac#-mattermost.iaa.ncsu.edu`) are not cloud services (they are operated by the IAA), and are special authorized exceptions. **Note that Gitlab.com is NOT allowed** because it is a cloud service.

12e.) Additional Software Requests

—Your Practicum Server account is a Standard account rather than an Administrator. You should not be installing any software by yourself (acceptable exceptions: installing R or Python packages). Request additional software from the HDS. Requests are usually granted. *Optional software is available to you on the Desktop in the Software Center app (e.g. LaTeX, JetBrains PyCharm...) and you are authorized to install anything available in Software Center.*

12f.) Maintenance Downtime

—There is a “Maintenance Window” periodically (schedule is “to be determined”) when the server reboots to install updates. During this Maintenance Window, you must assume the Practicum Server will reboot and log you off. Any work you were in the middle of will be stopped, so prepare for this accordingly.

—During the Maintenance Window, software updates will run for Windows, browsers, and other software. Under exceptional circumstances the Tech Lead can request that the Maintenance Window is postponed due to scheduling difficulty.

12g.) Web Browsing on the Practicum Server

—Do not browse the web on the Practicum Server except for legitimate uses. Avoid browsing at all if you can do it on your Student Laptop instead. Web browsing is inherently risky. Nearly every month Google patches vulnerabilities in Chrome that could allow infection to your practicum server by simply going to the wrong website.

12h.) Unauthorized Access to Practicum Server

—Do not allow anyone else to access/control your Practicum Server account, not even your Sponsor via online meeting remote control.

13.) Student Travel

13a.) Traveling to Present to the Sponsor In-Person

—If there is a need to carry Data for a Sponsor visit, talk to the Head of Data Security to ensure appropriate encryption and security measures are in place. It is common for the HDS to help you create an encrypted USB drive to take to the Sponsor, but do not copy data off the encrypted USB drive.

13b.) Traveling During Breaks / Holidays

—If you plan to do Practicum work when traveling...

Travel presents some unique risks, particularly with airport security and accessing the Internet from certain locations. Generally, if you plan to travel and remotely work on the Practicum, please discuss with the Head of Data Security first. Additionally, some Sponsors have data use restrictions (or language in the NDA) that prevents access to the Data from outside the United States. Read the NDA carefully. Talk to your sponsor if you plan to travel and work outside the US (e.g. over winter break.)

14.) Anticipated FAQ

14a.) *Who do I contact about problems with the Practicum?*

System Administrator (Brandon Barbour) – {general practicum server and technology concerns}

Head of Data Security (John Jernigan) – {data transfer, PII, security}

If Head of Data Security is unavailable, contact the System Administrator.

Practicum Manager (Dr. West) – {non-technological practicum issues}

Faculty and Teaching Assistants – {academic issues, performance techniques}

14b.) *(Printing capability has been removed as an available service.)*

14c.) *How can we shred paper documents?*

—Give the documents to the Head of Data Security for shredding. Be sure to indicate your Team Name for documentation purposes.

14d.) *How do we securely erase Sponsor Data?*

—First of all, you *can* delete normal Sponsor Data on your *Practicum Server* without any special instructions.

—At the end of the Practicum, the HDS will securely erase University-owned equipment. However, you will be asked to ensure there is no Practicum Data on your personal assets (e.g. Student Laptop, email account, Google Drive). There never should be Data on your personal assets, however.

—If the Sponsor accidentally sends personally-identifiable or financially sensitive data, ask the Head of Data Security for help immediately.

—If a mistake occurs, and you have Practicum Data on your Student Laptop, note that you must NOT attempt to delete Data yourself unless you are following instructions by the HDS. Improperly erased Sponsor Data cannot easily be securely erased later. Windows does not have built-in secure erasing capabilities, and third-party erasing software must be used. Securely erased Sponsor Data must be documented by the HDS.

14e.) What do we do if we detect the Sponsor has sent personally-identifiable information (PII) or financially-sensitive data by mistake?

—Contact the Head of Data Security immediately, and instruct the rest of your Practicum Team to NOT access the Practicum Server until the issue is resolved. The HDS will help you resolve the issue. The Sponsor will either need to re-transmit the Sponsor Data, or possibly at the Sponsor's and the HDS' discretion, the Sponsor Data may be cleaned by the Practicum Team.

14f.) How do we present content to our Sponsor or IAA Faculty?

—If you are at the IAA, you can connect to the Practicum Server through the VPN and Remote Desktop, then open any slides (e.g. Powerpoint) on the Practicum Server while it is in full-screen mode. Test this on a meeting room display, there may be glitches. You may instead request from the HDS **permission** to take an encrypted USB drive that can be presented on any computer. Do not copy presentation materials off the encrypted USB drive!

15.) Appendix A

Secure Password Guidelines (e.g. with Microsoft BitLocker encrypted USB drives)

A secure password is both difficult to guess, either mentally or computationally, and easy to remember. Always use strong passwords, and keep them well protected. When encrypting a USB drive with Microsoft BitLocker, the strength of the password is correlated to the strength of the encryption.

Note: the HDS will need to give you explicit permission to carry encrypted Data with you to an on-site presentation using Microsoft BitLocker, and will be involved in the process.

- **Ordinary passwords should be at least 10 characters.** Longer passwords are preferable to more randomness, if you had to choose.
- **Encryption passwords should be at least 15 characters.** Longer passwords are preferable to more randomness, if you had to choose.
- **Use uppercase, lowercase, and ideally symbols/numerals.** This can make it harder for attackers to determine.
- **Optionally, think of phrases or sequences of words, provided they're not obvious! These will be easier to remember and type!**
 - e.g. **QueenBee-TwelveJokers** ...or... **Winding road, mountain air**
- **Weaker passwords:** 'purple5', '09281967', 'adams318' (these are short with little complexity regarding uppercase, lowercase, numerals, and symbols, and a brute-force attempt on these passwords will succeed quickly with modern computing capability)
- **Stronger passwords:** **products*PERU*panama** ...or... **Austin limits: cold Colorado**

16.) Appendix B

Monthly Student Laptop Checkups

In order to ensure your laptop (and any secondary desktop/laptop computer) is in compliance with this policy, once per month the HDS will announce the date of a device security check.

You will have approximately 1 week's notice to ensure that specific security controls are met, such as applying Windows or macOS updates, web browser updates, and antivirus scans. On the date and time of the security check, students will be required to submit screenshots proving compliance in the mentioned security controls. All students are expected to be in compliance.

Failure to submit the screenshots by the announced deadline will result in your name being sent to Dr. Rappa and faculty as a violation of practicum security policy. Your access to the Practicum Server will be disabled until the screenshots are submitted, and followup discussion with the HDS is resolved.