Data Security Policy for Research Projects Involving Human Subjects

Contents

1.0 Overview

This policy outlines the protection of research data at the University of Northern Colorado. The policy defines various information security classification levels and adequate security measures must be taken to protect research data at each classification level.

2.0 Purpose

Personally identifiable data collected for, used in, or resulting from research involving human subjects must be protected from inadvertent or inappropriate disclosure. While the responsibility for protecting research data ultimately rests with researchers, this procedure ensures the correct security measures have been considered and appropriately implemented using state-of-the-art security measures available at the University of Northern Colorado.

3.0 Scope

This policy applies to any individual (faculty, student, or staff) working on a research project as part of their affiliation with the University of Northern Colorado and collecting, receiving, transmitting, or storing personally identifiable data.

4.0 Definitions, Roles, and Requirements

Investigators:

- ✓ Review the five levels of data security and consider applicability for information the researcher will collect, transmit, receive, etc.
- ✓ If any research data is anticipated to be level 3, 4, or 5 data (see below for definitions of each level), disclose the nature of the data they intend to work with and/or collect so the Investigator and the CISO (or an individual designated by the CISO) are able to confirm the data security risk
- ✓ Prepare data security plan in accordance with classification level of the data if the level has been confirmed to be level 3, 4, or 5
- ✓ Implement and monitor the data security plans over the duration of the project

Chief Information Officer (CISO):

- ✓ May delegate any portion of the items in this document specified for the CISO to another individual
- ✓ Ensures the adequacy of protection plans to maintain the confidentiality and integrity of research data
- ✓ Obtains the assurance of the Investigator via the signature page located in Appendix F below confirming that the requirements outlined in the *University of Northern Colorado Data Security Policy for Research Projects* for the applicable classification level will be followed
- ✓ May approve variances from the security requirements for the applicable classification level that would apply to data so long as the resulting study data security plan complies with any legal requirements
- ✓ May seek the advice and recommendations of others qualified in assessing the adequacy of protection for the data and in assessing the appropriate data classification level

Research: Federal regulation 45 CFR 46 defines research as "a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge."

Human Subjects: Federal regulation 45 CFR 46 defines a human subject as, "a living individual about whom an investigator (whether professional or student) conducting research obtains (1) Data through intervention or interaction with the individual, or (2) Identifiable private information." According to the University Regulations 3-8-104 (http://www.unco.edu/trustees/University_Regulations.pdf) research with human participants must be reviewed and approved by the Institutional Review Board (IRB) prior to data collection. The IRB website is located at http://www.unco.edu/osp/ethics/irb/. In cases in which a data agreement plan is required or the researcher will have access to especially sensitive data about people, which if inadvertently disclosed, would put these individuals at serious risk (see Levels 3, 4, and 5 below), a data security plan must be reviewed and approved by the CISO (or an individual designated by the CISO) before the investigator collects, receives, transmits, or otherwise gains access to the data (see final page of this document). It is acceptable for the researcher to submit the data security plan and the IRB application concurrently.

5.0 Sources of Data

Research Data Sources or Research Facilities External to the University of Northern Colorado

Some research data come from sources external to the University of Northern Colorado. Such data are often protected by an agreement (such as a data use or business agreement) that defines use limitations and/or protection requirements for the data. Individuals working with such data must comply with the use limits and protection requirements in the use agreement. If data are subject to security requirements specified in an information use agreement, grant, or contract, those requirements must be met.

Individuals using facilities external to the University of Northern Colorado, such as hospitals, are subject to the security policies in force at such facilities. Note that the research may be covered by the policies of

both the University of Northern Colorado and the external facility. In the event that the external facility lacks an applicable policy, the research data should be protected under the University of Northern Colorado's policies.

Only individuals that have been specifically authorized to sign an information agreement on behalf of the University may sign such agreements, even when the agreements do not include any transfers of funds. Authorized individuals include the Vice President and General Counsel (VPGC), Assistant Vice President for Research (AVPR), and the CISO, or individuals specifically designated by the VPGC, AVPR, or the CISO.

Research Data from the University of Northern Colorado Sources

Researchers often deal with sensitive data that can relate to or emanate from human beings, include proprietary information, access information that has national security implications, etc. Such data should be classified to the appropriate level and protected accordingly as outlined below.

6.0 Classification of Research Data

The University of Northern Colorado has specific security requirements for research data classified in any of the categories listed below. Please note that data assessed at a lower security level does not necessarily indicate unimportant repercussions from a security breach. Detailed security requirements pertaining to each security level are found in the appendices of this policy. Thus, researchers are advised to be cautious with all personally identifiable information.

Level 1 - De-identified research information about people and other non-confidential research data
Research data in which all information that could be used directly or indirectly to identify an individual has been removed or modified. Federal IRB regulations describe such data as information "recorded by the investigator in such a manner that subjects cannot be identified, directly or through identifiers linked to the subjects." The HIPAA Privacy Rule for protected health information specifies eighteen categories of information that must be removed in order to de-identify data. There are no specific University requirements for the protection of de-identified research information or for other non-confidential research information, but researchers need to seek approval for applicable research through the IRB and will to protect such data as a matter of responsible practice.

Level 2 – Mildly sensitive or confidential information about individually identifiable people

- Individually identifiable information which if disclosed would not ordinarily be expected to result in material harm, but as to which a subject has been promised specific procedures for protecting confidentiality.
- Individually identifiable information that is not protected by law (e.g. HIPAA or FERPA)
- Sensitive information that could be embarrassing if disclosed, such as interviews or questionnaires about personal issues.

Level 3 - Legally protected sensitive information about individually identifiable people

Individually identifiable information that if disclosed could reasonably be expected to be damaging to a person's reputation or to violate his or her legal rights to privacy. Such data could include, but is not limited to:

- Student record information protected by FERPA (Family Educational Rights and Privacy Act). Information regarding FERPA can be found at: http://www2.ed.gov/policy/gen/guid/fpco/index.html.

Level 4 - Very sensitive information about individually identifiable people

Individually identifiable high risk confidential data that if disclosed cause a non-minimal risk of civil liability, moderate psychological harm, or material social harm to individuals or groups including, but not limited to:

- Social Security numbers
- Medical records that are not categorized as extremely sensitive as outlined in Level 5 requirements above
- Individually identifiable financial information
- Medical records may also be subject to Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations. For more information on HIPAA relating to research purposes, visit http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/research/research.pdf
- Subject to specific government requirements in each case, sensitive national security information should usually be classified as Level 4 information

Level 5 - Extremely sensitive data about individually identifiable people

Individually identifiable data that if disclosed could cause significant harm to an individual if exposed, including, but not limited to:

- Serious risk of criminal liability
- Serious psychological harm or other significant injury
- Loss of insurability or employability
- Significant social harm to an individual or group

7.0 Legal Requests for Research Information

On occasion, a researcher will receive a subpoena, national security request or court order demanding disclosure of information in their possession. Should this occur, the researcher must tell the person making the request to contact the University of Northern Colorado's Legal Counsel. No other individuals are authorized to respond to these types of requests. The researcher must advise one of the IRB co-chairs.

To guard against the compelled disclosure of research data containing individually identifiable data, researchers should consider obtaining applicable government-provided protections for certain kinds of data. For example, research may qualify for a Certificate of Confidentiality. A Certificate of Confidentiality will allow a researcher to refuse to disclose personally identifiable data concerning research subjects in civil, criminal, administrative, legislative or other proceedings. Such subjects can be protected if the research data could damage their financial standing, employability, insurability or reputation. Certificates of Confidentiality can be obtained from the NIH for NIH funded research. (See https://humansubjects.nih.gov/coc/index for more information). The Department of Justice also may grant similar protections for research involving criminal records. Research funded by the federal Agency for Health Care Policy and Research is offered a form of automatic protection. Investigators should consult the University of Northern Colorado's legal counsel and IRB co-chairs for further information on obtaining these protections.

8.0 Enforcement

Violation of this policy may result in disciplinary action under appropriate University disciplinary procedures for employees, faculty, and staff. Legal consequences through law enforcement may also apply to any individual who violates state or federal law.

9.0 Signature of Attestation

The Signature of Attestation sheet is required to be filled out and signed by this policy. This form can be found in Appendix F of this policy.

10.0 Revision History

Version	Date	Editor	Nature of Change
1.0	11/14/2012	Jessica Behunin	Initial Draft
1.1	4/15/2013	Jessica Behunin	Official release and minor edits
1.2	5/23/2013	Jessica Behunin	Minor content edits
1.3	7/12/2013	Jessica Behunin	Minor content edits
1.4	9/12/2013	Forrest H. Swick	Minor formatting
1.5	9/11/2014	Matt Langford	Minor content edits
1.6	1/2/2018	Forrest H. Swick	Minor content edits

11.0 Appendices

Appendices A through E outline the security requirements for each level of data identified via the policy contained in this document.

Appendix A: Level 1 Security Requirements

There are no specific University requirements for the protection of de-identified research information or for other non-confidential research information except that the researcher must apply for IRB approval for all applicable data collection.

Appendix B: Level 2 Security Requirements

The following requirements are applicable to any computer and/or server that will be used in the handling of research data identified at a Level 2:

1. **Generic accounts must be disabled.** A generic account is any account used to logon to a computer or server that is not tied to a specific user and is shared by more than one person. Example: All researchers are logging in to a computer using a username of RESEARCHERS and the same shared password.
2. **Users must have access to the computers and/or servers via individual user accounts and not shared accounts.** Example: John Smith logs on to a computer with a username and password that only he knows.
3. **Passwords must follow the University policy regarding complexity.** The policy can be found at http://www.unco.edu/information-management-technology/about-us/standards_policies_procedures.aspx. This is to ensure that passwords are difficult to guess, thus making access for unauthorized individuals difficult.
4. **Default passwords on computers and/or servers must be changed prior to housing any research data.** A default password is one that is typically shipped with a computer or server to allow for initial setup of the equipment. Example: When receiving a new computer from the manufacturer, instructions indicate to logon to the computer using **admin** as the username and password.
5. **Initial passwords assigned to individual users must be set to require the user to change it at their first login.** Administrators must provide access to users. As such, they are given a username and password that both the administrator and the user know. By forcing the user to change their password the first time they use it, this allows the user to then have a password that is known only to the user.
6. **When users no longer need access to the data, computers, and/or servers used for the specified research project, their user accounts must be removed with a sense of urgency.** It is easy to forget when people leave the University or transfer to other departments that they still have access to systems which they no longer need access to.
7. **Failed logon attempts will lock the computer or server out after 3 attempts.** When logging on to a computer, someone with malicious intent may attempt to guess the username and password on a computer. Changing the settings to lock the computer out after 3 failed attempts prevents an attacker from being able to guess as many times as they would like.
8. **Enable a screen saver to activate after 15 minutes of inactivity that requires a password to unlock the computer or server.** People often walk away from a computer forgetting to lock the screen (using ctrl-alt-delete, or Windows Key+L). This leaves access wide open to people passing by. This setting will enable a screen saver after 15 minutes of a researcher not using a PC that requires a password to unlock the computer when the researcher is ready to resume use.
9. **Users of the computers and/or servers involved in the research project must be educated regarding suspected security incident handling procedures.** If a researcher suspects that data has been put at risk, they are to immediately report this to the IRB and the IM&T CISO. This is to ensure proper containment and recovery from the potential incident.

10. **Individuals who are working with sensitive research data identified as Levels 3-5 will be required to take UNC's online Information Security Training Course offered through Skillsoft, or be trained in person by a member of UNC's IM&T Security Team.** Technology is a constantly changing world, and information security is critical when dealing with research data. As such, each individual who is involved with research data will receive information security training at a minimum of annually and will sign off as having done so.
11. **In the event of a suspected security incident, system logs must be reviewed by the IM&T Security Team.** Should an incident occur where an unauthorized individual gains access to data, or an authorized individual treats the data inappropriately, IM&T staff are trained to be able to gather the necessary information to properly resolve the security incident and reduce the risk of future incidents.
12. **Antivirus software must be installed and running on computers or servers and set to update itself to the latest version at a minimum of weekly.** Malicious software such as viruses and worms create a major threat to computers and servers. As such, it is important to have antivirus software running at all times. Since such threats are constantly changing, it is critical to have the software set up to receive updates at a minimum of weekly.
13. **All system access must be logged by the computers and/or servers being used for research purposes.** Logs are used to identify activity on a computer or server. This helps identify what actions were taken by individual users and at what time. Logs must include the user's identity, the action the user took, and the time the action was taken by the user.
14. **System patches applicable to research computers and/or servers must be kept up to date.** When patches are released by manufacturers such as Microsoft, they are typically to repair a security weakness in a system. As such, computers and/or servers used for research purposes must have patches in place to ensure the security of the system remains intact.
15. **University owned systems should be scanned at a minimum of annually for security vulnerabilities.** This helps ensure that the risk of exposure of research data is minimized and that sensitive information is being handled in a secure manner.
16. **Implementation of requirements is subject to review and audit by the Office of Information Security, IM&T, and/or the IRB.**

Appendix C: Level 3 Security Requirements

The following requirements are applicable to any computer and/or server that will be used in the handling of research data identified at a Level 3:

1. **Generic accounts must be disabled.** A generic account is any account used to logon to a computer or server that is not tied to a specific user and is shared by more than one person. Example: All researchers are logging in to a computer using a username of RESEARCHERS and the same shared password.
2. **Users must have access to the computers and/or servers via individual user accounts and not shared accounts.** Example: John Smith logs on to a computer with a username and password that only he knows.
3. **Passwords must follow the University policy regarding complexity.** The policy can be found at http://www.unco.edu/information-management-technology/about-us/standards_policies_procedures.aspx. This is to ensure that passwords are difficult to guess, thus making access for unauthorized individuals difficult.
4. **Default passwords on computers and/or servers must be changed prior to housing any research data.** A default password is one that is typically shipped with a computer or server to allow for initial setup of the equipment. Example: When receiving a new computer from the manufacturer, instructions indicate to logon to the computer using **admin** as the username and password.
5. **Initial passwords assigned to individual users must be set to require the user to change it at their first login.** Administrators must provide access to users. As such, they are given a username and password that both the administrator and the user know. By forcing the user to change their password the first time they use it, this allows the user to then have a password that is known only to the user.
6. **When users no longer need access to the data, computers, and/or servers used for the specified research project, their user accounts must be removed with a sense of urgency.** It is easy to forget when people leave the University or transfer to other departments that they still have access to systems which they no longer need access to.
7. **Failed logon attempts will lock the computer or server out after 3 attempts.** When logging on to a computer, someone with malicious intent may attempt to guess the username and password on a computer. Changing the settings to lock the computer out after 3 failed attempts prevents an attacker from being able to guess as many times as they would like.
8. **Enable a screen saver to activate after 10 minutes of inactivity that requires a password to unlock the computer or server.** People often walk away from a computer forgetting to lock the screen (using ctrl-alt-delete, or Windows Key+L). This leaves access wide open to people passing by. This setting will enable a screen saver after 10 minutes of a researcher not using a PC that requires a password to unlock the computer when the researcher is ready to resume use.
9. **Users of the computers and/or servers involved in the research project must be educated regarding suspected security incident handling procedures.** If a researcher suspects that data has been put at risk, they are to immediately report this to the IRB and the IM&T CISO. This is to ensure proper containment and recovery from the potential incident.

10. **Individuals who are working with sensitive research data identified as Levels 3-5 will be required to take UNC's online Information Security Training Course offered through Skillsoft, or be trained in person by a member of UNC's IM&T Security Team.** Technology is a constantly changing world, and information security is critical when dealing with research data. As such, each individual who is involved with research data will receive information security training at a minimum of annually and will sign off as having done so.
11. **In the event of a suspected security incident, system logs must be reviewed by the IM&T Security Team.** Should an incident occur where an unauthorized individual gains access to data, or an authorized individual treats the data inappropriately, IM&T staff are trained to be able to gather the necessary information to properly resolve the security incident and reduce the risk of future incidents.
12. **Antivirus software must be installed and running on computers or servers and set to update itself to the latest version at a minimum of weekly.** Malicious software such as viruses and worms create a major threat to computers and servers. As such, it is important to have antivirus software running at all times. Since such threats are constantly changing, it is critical to have the software set up to receive updates at a minimum of weekly.
13. **All system access must be logged by the computers and/or servers being used for research purposes.** Logs are used to identify activity on a computer or server. This helps identify what actions were taken by individual users and at what time. Logs must include the user's identity, the action the user took, and the time the action was taken by the user.
14. **System logs will be periodically reviewed by IM&T Security staff for evidence of systems under attack or for unauthorized actions taken by authorized users.** This ensures that the security of the system remains at the appropriate level to reduce the risk of malicious activity both from the inside and the outside perspectives.
15. **System patches applicable to research computers and/or servers must be kept up to date.** When patches are released by manufacturers such as Microsoft, they are typically to repair a security weakness in a system. As such, computers and/or servers used for research purposes must have patches in place to ensure the security of the system remains intact.
16. **University owned systems should be scanned at a minimum of annually for security vulnerabilities.** This helps ensure that the risk of exposure of research data is minimized and that sensitive information is being handled in a secure manner.
17. **Systems must not be directly accessible from the internet or from open parts of UNC's network. Connecting using the secure VPN is considered safe and is permitted.** This reduces the risk of the data being accessed by unauthorized individuals.
18. **Sensitive information must be encrypted when it is transmitted to or from any systems by electronic means.** Data must be protected when it is transmitted to prevent unauthorized access.
19. **Sensitive data must never be sent via email unless the information has been encrypted.** Email communications are no more secure than writing information on a postcard and sending it through the mail for anybody to see. Encrypting the files protects them from unauthorized access.
20. **Systems connected to any network must run a host-based firewall configured to block all connections to the system other than the specific types of connections needed to perform the approved research. Configurations to the host-based firewall must be set up and maintained**

by IM&T staff. This reduces the risk again of an external entity gaining unauthorized access to the data.

21. **Implementation of requirements is subject to review and audit by the Office of Information Security, IM&T, and/or the IRB.**
22. **All external media containing sensitive data must be adequately secured via physical locks, encryption, etc. when not in use.** Examples of external media include, but are not limited to CDs, thumb drives, flash drives, USB drives, external hard drives, paper records, etc.
23. **In cases where access to systems containing sensitive data from outside the research premises is permitted, there must be a signed acknowledgement of proper security controls in place by the IM&T CIO prior to allowing that access.**
24. **The IRB must be informed and approve of any plans to have a vendor store or process sensitive information.**
25. **Contracts must be executed with all external vendors who process or store sensitive information at UNC's direction.** The contracts must contain specific language that requires a vendor to protect the confidential information and to inform UNC's IM&T CISO immediately of any suspected breach or risk of exposure has been identified.
26. **Only the applications required to support the required services can be running on a system.** This basically means that the computers and/or servers are not to be used to run other programs not needed for the research or protection of the data. An example of this might be installing a screen saver software from the internet that creates a photo slide show on the PC.
27. **Collection of Level 3 information while in the field must adhere to strict security protocols.** The protocol(s) that will be used must be provided to the IRB. Examples may include:
    a. Computer-based collection of Level 3 information in the field is done using a VPN connection to a Level 3 server.
    b. Computer-based collection of Level 3 information in the field may be done using a computer with an encrypted disk. Information collected in the field must be transferred by secure means to systems that meet Level 3 protection standards at the earliest opportunity, and then promptly, securely, and permanently deleted from the field service device (such as laptop, digital recorder, etc.).

Appendix D: Level 4 Security Requirements

The following requirements are applicable to any computer and/or server that will be used in the handling of research data identified at a Level 4:

1. **Generic accounts must be disabled.** A generic account is any account used to logon to a computer or server that is not tied to a specific user and is shared by more than one person. Example: All researchers are logging in to a computer using a username of RESEARCHERS and the same shared password.
2. **Users must only have access to the computers and/or servers via individual user accounts and not shared accounts.** Example: John Smith logs on to a computer with a username and password that only he knows.
3. **Passwords must follow the University policy regarding complexity.** The policy can be found at http://www.unco.edu/information-management-technology/about-us/standards_policies_procedures.aspx. This is to ensure that passwords are difficult to guess, thus making access for unauthorized individuals difficult.
4. **Default passwords on computers and/or servers must be changed prior to housing any research data.** A default password is one that is typically shipped with a computer or server to allow for initial setup of the equipment. Example: When receiving a new computer from the manufacturer, instructions indicate to logon to the computer using **admin** as the username and password.
5. **Initial passwords assigned to individual users must be set to require the user to change it at their first login.** Administrators must provide access to users. As such, they are given a username and password that both the administrator and the user know. By forcing the user to change their password the first time they use it, this allows the user to then have a password that is known only to the user.
6. **When users no longer need access to the data, computers, and/or servers used for the specified research project, their user accounts must be removed with a sense of urgency.** It is easy to forget when people leave the University or transfer to other departments that they still have access to systems which they no longer need access to.
7. **Failed logon attempts will lock the computer or server out after 3 attempts.** When logging on to a computer, someone with malicious intent may attempt to guess the username and password on a computer. Changing the settings to lock the computer out after 3 failed attempts prevents an attacker from being able to guess as many times as they would like.
8. **Enable a screen saver to activate after 10 minutes of inactivity that requires a password to unlock the computer or server.** People often walk away from a computer forgetting to lock the screen (using ctrl-alt-delete, or Windows Key+L). This leaves access wide open to people passing by. This setting will enable a screen saver after 10 minutes of a researcher not using a PC that requires a password to unlock the computer when the researcher is ready to resume use.
9. **Users of the computers and/or servers involved in the research project must be educated regarding suspected security incident handling procedures.** If a researcher suspects that data

has been put at risk, they are to immediately report this to the IRB and the IM&T CISO. This is to ensure proper containment and recovery from the potential incident.

10. **Individuals who are working with sensitive research data identified as Levels 3-5 will be required to take UNC's online Information Security Training Course offered through Skillsoft, or be trained in person by a member of UNC's IM&T Security Team.** Technology is a constantly changing world, and information security is critical when dealing with research data. As such, each individual who is involved with research data will receive information security training at a minimum of annually and will sign off as having done so.
11. **In the event of a suspected security incident, system logs must be reviewed by the IM&T Security Team.** Should an incident occur where an unauthorized individual gains access to data, or an authorized individual treats the data inappropriately, IM&T staff are trained to be able to gather the necessary information to properly resolve the security incident and reduce the risk of future incidents.
12. **Antivirus software must be installed and running on computers or servers and set to update itself to the latest version at a minimum of weekly.** Malicious software such as viruses and worms create a major threat to computers and servers. As such, it is important to have antivirus software running at all times. Since such threats are constantly changing, it is critical to have the software set up to receive updates at a minimum of weekly.
13. **All system access must be logged by the computers and/or servers being used for research purposes.** Logs are used to identify activity on a computer or server. This helps identify what actions were taken by individual users and at what time. Logs must include the user's identity, the action the user took, and the time the action was taken by the user.
14. **System logs will be periodically reviewed by IM&T Security staff for evidence of systems under attack or for unauthorized actions taken by authorized users.** This ensures that the security of the system remains at the appropriate level to reduce the risk of malicious activity both from the inside and the outside perspectives.
15. **System patches applicable to research computers and/or servers must be kept up to date.** When patches are released by manufacturers such as Microsoft, they are typically to repair a security weakness in a system. As such, computers and/or servers used for research purposes must have patches in place to ensure the security of the system remains intact.
16. **University owned systems should be scanned at a minimum of annually for security vulnerabilities.** This helps ensure that the risk of exposure of research data is minimized and that sensitive information is being handled in a secure manner.
17. **Systems must not be directly accessible from the internet or from open parts of UNC's network.** Connecting using the secure VPN is considered safe and is permitted. This reduces the risk of the data being accessed by unauthorized individuals.
18. **Sensitive information must be encrypted when it is transmitted to or from any systems by electronic means.** Data must be protected when it is transmitted to prevent unauthorized access.
19. **Sensitive data must never be sent via email unless the information has been encrypted.** Email communications are no more secure than writing information on a postcard and sending it through the mail for anybody to see. Encrypting the files protects them from unauthorized access.

20. **Systems connected to any network must run a host-based firewall configured to block all connections to the system other than the specific types of connections needed to perform the approved research. Configurations to the host-based firewall must be set up and maintained by IM&T staff.** This reduces the risk again of an external entity gaining unauthorized access to the data.
21. **Implementation of requirements is subject to review and audit by the Office of Information Security, IM&T, and/or the IRB.**
22. **All external media containing sensitive data must be adequately secured via physical locks, encryption, etc. when not in use.** Examples of external media include, but are not limited to CDs, thumb drives, flash drives, USB drives, external hard drives, paper records, etc.
23. **In cases where access to systems containing sensitive data from outside the research premises is permitted, there must be a signed acknowledgement of proper security controls in place by the IM&T CIO prior to allowing that access.**
24. **Sensitive information is restricted from being stored on any computer or portable electronic device unless the sensitive information is encrypted.** Examples of portable electronic devices include, but are not limited to smartphones, iPads, laptops, etc.
25. **The IRB must be informed and approve of any plans to have a vendor store or process sensitive information.**
26. **Contracts must be executed with all external vendors who process or store sensitive information at UNC's direction.** The contracts must contain specific language that requires a vendor to protect the confidential information and to inform UNC's IM&T CISO immediately of any suspected breach or risk of exposure has been identified.
27. **Only the applications required to support the required services can be running on a system.** This basically means that the computers and/or servers are not to be used to run other programs not needed for the research or protection of the data. An example of this might be installing a screen saver software from the internet that creates a photo slide show on the PC.
28. **Collection of Level 4 information while in the field must adhere to strict security protocols.** The protocol(s) that will be used must be provided to the IRB. Examples may include:
    a. Computer-based collection of Level 4 information in the field is done using a VPN connection to a Level 4 server.
    b. Computer-based collection of Level 4 information in the field may be done using a computer with an encrypted disk. Information collected in the field must be transferred by secure means to systems that meet Level 4 protection standards at the earliest opportunity, and then promptly, securely, and permanently deleted from the field service device (such as laptop, digital recorder, etc.).
29. **Systems must be located only in a physically secure area under UNC's control.**
30. **UNC's CISO must provide written authorization prior to connecting systems to the network.**
31. **Systems must be only connected to a special network segment dedicated to similar systems which are assigned private address space addresses.** This must be coordinated through IM&T.
32. **No computers that have not been certified to meet Level 4 requirements can reside on the aforementioned network segment.**

33. **The aforementioned network segment must be protected by a firewall that is configured to block all inbound traffic from systems not specifically required to support the application.** Outbound traffic must also be blocked from the system to any destination not specifically required to support the application. This must be coordinated through IM&T.
34. **The firewall protecting the network segment with the systems must block all administrator access except from the specific systems used by the system administrators.**
35. **Systems connected to any network must run host-based firewalls configured to block all connections to the system other than the specific types of connections needed to perform the approved research.**
36. **There must be a written list of the individuals that are permitted to have accounts on the system.** This list must be provided to the head of the research project.
37. **Backups of any confidential information must follow the same security requirements as if it were the original.**
38. **Disposal of confidential data must be done by adequate physical destruction of the data.**

Appendix E: Level 5 Security Requirements

The following requirements are applicable to any computer and/or server that will be used in the handling of research data identified at a Level 5:

1. **Generic accounts must be disabled.** A generic account is any account used to logon to a computer or server that is not tied to a specific user and is shared by more than one person. Example: All researchers are logging in to a computer using a username of RESEARCHERS and the same shared password.
2. **Users must only have access to the computers and/or servers via individual user accounts and not shared accounts.** Example: John Smith logs on to a computer with a username and password that only he knows.
3. **Passwords must follow the University policy regarding complexity.** That policy can be found at http://www.unco.edu/information-management-technology/about-us/standards_policies_procedures.aspx. This is to ensure that passwords are difficult to guess, thus making access for unauthorized individuals difficult.
4. **Default passwords on computers and/or servers must be changed prior to housing any research data.** A default password is one that is typically shipped with a computer or server to allow for initial setup of the equipment. Example: When receiving a new computer from the manufacturer, instructions indicate to logon to the computer using **admin** as the username and password.
5. **Initial passwords assigned to individual users must be set to require the user to change it at their first login.** Administrators must provide access to users. As such, they are given a username and password that both the administrator and the user know. By forcing the user to change their password the first time they use it, this allows the user to then have a password that is known only to the user.
6. **When users no longer need access to the data, computers, and/or servers used for the specified research project, their user accounts must be removed with a sense of urgency.** It is easy to forget when people leave the University or transfer to other departments that they still have access to systems which they no longer need access to.
7. **Failed logon attempts will lock the computer or server out after 3 attempts.** When logging on to a computer, someone with malicious intent may attempt to guess the username and password on a computer. Changing the settings to lock the computer out after 3 failed attempts prevents an attacker from being able to guess as many times as they would like.
8. **Enable a screen saver to activate after 5 minutes of inactivity that requires a password to unlock the computer or server.** People often walk away from a computer forgetting to lock the screen (using ctrl-alt-delete, or Windows Key+L). This leaves access wide open to people passing by. This setting will enable a screen saver after 10 minutes of a researcher not using a PC that requires a password to unlock the computer when the researcher is ready to resume use.
9. **Users of the computers and/or servers involved in the research project must be educated regarding suspected security incident handling procedures.** If a researcher suspects that data has been put at risk, they are to immediately report this to the IRB and the IM&T CISO. This is to ensure proper containment and recovery from the potential incident.

10. **Individuals who are working with sensitive research data identified as Levels 3-5 will be required to take UNC's online Information Security Training Course offered through Skillsoft, or be trained in person by a member of UNC's IM&T Security Team.** Technology is a constantly changing world, and information security is critical when dealing with research data. As such, each individual who is involved with research data will receive information security training at a minimum of annually and will sign off as having done so.
11. **In the event of a suspected security incident, system logs must be reviewed by the IM&T Security Team.** Should an incident occur where an unauthorized individual gains access to data, or an authorized individual treats the data inappropriately, IM&T staff are trained to be able to gather the necessary information to properly resolve the security incident and reduce the risk of future incidents.
12. **Antivirus software must be installed and running on computers or servers and set to update itself to the latest version at a minimum of daily.** Malicious software such as viruses and worms create a major threat to computers and servers. As such, it is important to have antivirus software running at all times. Since such threats are constantly changing, it is critical to have the software set up to receive updates at a minimum of daily.
13. **All system access must be logged by the computers and/or servers being used for research purposes.** Logs are used to identify activity on a computer or server. This helps identify what actions were taken by individual users and at what time. Logs must include the user's identity, the action the user took, and the time the action was taken by the user.
14. **System logs will be reviewed daily by IM&T Security staff for evidence of systems under attack or for unauthorized actions taken by authorized users.** This ensures that the security of the system remains at the appropriate level to reduce the risk of malicious activity both from the inside and the outside perspectives.
15. **System patches applicable to research computers and/or servers must be kept up to date if systems are connected to the network at any point.** When patches are released by manufacturers such as Microsoft, they are typically to repair a security weakness in a system. As such, computers and/or servers used for research purposes must have patches in place to ensure the security of the system remains intact.
16. **University owned systems should be scanned at a minimum of annually for security vulnerabilities.** This helps ensure that the risk of exposure of research data is minimized and that sensitive information is being handled in a secure manner.
17. **Sensitive information must be encrypted when it is transmitted to or from any systems by electronic means.** Data must be protected when it is transmitted to prevent unauthorized access.
18. **Sensitive data must never be sent via email unless the information has been encrypted.** Email communications are no more secure than writing information on a postcard and sending it through the mail for anybody to see. Encrypting the files protects them from unauthorized access.
19. **If connected to the network, the connection must be protected by a firewall that is configured by the appropriate IM&T staff.** This firewall will be configured to block all inbound traffic from systems not specifically required to support the applications. Outbound traffic must also be blocked from the system to any destination not specifically required to support the applications.

20. **Implementation of requirements is subject to review and audit by the Office of Information Security, IM&T, and/or the IRB.**
21. **All external media containing sensitive data must be encrypted and locked in a safe which is in a physically secure room when not in use.** The names of the specific people who have access to the media must be provided to the project lead. Examples of external media include, but are not limited to CDs, thumb drives, flash drives, USB drives, external hard drives, paper records, etc.
22. **In cases where access to systems containing sensitive data from outside the research premises is permitted, there must be a signed acknowledgement of proper security controls in place by the IM&T CISO prior to allowing that access.**
23. **Sensitive information is restricted from being stored on any computer or portable electronic device.** Examples of portable electronic devices include, but are not limited to smartphones, iPads, laptops, etc. This data must be stored on and used only in one or more physically secure rooms located in UNC controlled locations that meet Level 5 security requirements.
24. **All media (including non-electronic media) containing Level 5 information must not be removed from the secure room(s) unless written approval has been obtained by the project lead.**
25. **The IRB must be informed and approve of any plans to have a vendor store or process sensitive information.**
26. **Contracts must be executed with all external vendors who process or store sensitive information at UNC's direction.** The contracts must contain specific language that requires a vendor to protect the confidential information and to inform UNC's IM&T CISO immediately of any suspected breach or risk of exposure has been identified.
27. **Only the applications required to support the required services can be running on a system.** This basically means that the computers and/or servers are not to be used to run other programs not needed for the research or protection of the data. An example of this might be installing a screen saver software from the internet that creates a photo slide show on the PC.
28. **Collection of Level 5 information while in the field must adhere to strict security protocols.** The protocol(s) that will be used must be provided to the IRB. Examples may include:
    a. Computer-based collection of Level 5 information in the field may only be by saving collected information to an encrypted disk or encrypted thumb drive.
    b. Level 5 information collected in the field must be transferred by secure means to secure systems that meet Level 5 protection standards at the earliest opportunity, and then promptly, securely, and permanently deleted from the source device.
29. **Systems must be located in one or more physically secured rooms located in UNC controlled locations.** The secure rooms do not have to be dedicated to a specific Level 5 project.
30. **The room(s) must have entry/exit points that are controlled.**
31. **The interior of the room should not be visible from outside the building if it is on the ground floor via windows.**
32. **The project lead must be provided with a list of the individuals who will be permitted to have unescorted physical access to the room(s).** Other visitors to the secure area are only permitted in special circumstances (e.g., health emergencies, IT support and security reviews). Such visitors must be escorted at all times and their actions must be monitored.

33. **Individual access to the secure area must be captured and logged** (e.g., badge readers upon entry, security cameras, etc.).
34. **The log of physical access must be protected and restricted from unauthorized access.**
35. **The room must be prohibited from access via a universal, master, sub-master, or janitor key.**
36. **Any network connected to a Level 5 system must be localized and must not extend outside the secure room(s**). If there are multiple rooms, network connections between rooms must be protected by electrical conduit unless the rooms are adjacent.
37. **UNC's CISO must provide written authorization prior to connecting systems to the network.**
38. **There must be a written list of the individuals that are permitted to have accounts on the system.** This list must be provided to the head of the research project.
39. **Backups of any confidential information must follow the same security requirements as if it were the original.**
40. **Disposal of confidential data must be done by adequate physical destruction of the data.**
41. **No system on a network that connects to a Level 5 system may be accessible from outside the secure room(s) by any means.**
42. **No wireless network capabilities can be enabled on any Level 5 system.**
43. **No remote access capability can be enabled on any Level 5 system.**
44. **Level 5 systems should be dedicated to the single purpose of processing or storing Level 5 information.**
45. **Level 5 systems or backups may not be removed from the secure room(s) unless any storage disks in the system have been properly cleaned by physically destroying any hardware where Level 5 information has been stored.** IM&T should be contacted for proper destruction methods.
46. **No users' individual computers can reside on the same network segment as a Level 5 system.**
47. **The firewall protecting the network segment with the systems must block all administrator access except from the specific systems used by the system administrators.**

Appendix F: University of Northern Colorado Data Security Policy for Research Projects-Signature Page

The University of Northern Colorado's *Data Security Policy for Research Projects* is in place to ensure that research data is adequately protected. Please review the policy, then confirm the following security requirements below, initial and sign where indicated.

1. If your research is subject to a data use agreement (DUA):
    a. Please attach the security requirements in the DUA to this document.
    b. Certify that the specific requirements in the DUA can be met in your research facility or that the research will take place in a facility which has been previously certified to meet the security requirements in the DUA.
2. If your research data contains identifiable information and according to your analysis represents Level 3, 4, or 5:
    a. Using the "University of Northern Colorado Data Security for Research Projects Procedure," identify the appropriate classification level for the data and indicate here:

        Assessed Data Classification Level: _____

By initialing each line and signing below, you certify:

_____ The requirements in the "University of Northern Colorado Data Security for Research Projects Policy," for the above specified level of data can and will be met in your facility, or that your research will be done in a previously certified facility with standards applicable to the level of data referenced.

_____ You have provided a complete list of people (e.g. researchers and lab assistants) as well as the categories of people (IT support, etc.) with access to the research data and/or facility.

_____ You agree to promptly disable access to the research data for anyone who no longer needs access to the data due to a change in responsibility, those who are no longer employees of the University, etc.

_____ If remote access to the research data is required and allowed, you have provided a list of the individuals who will have access from off University premises and the reason for their access. Remote access will also be promptly removed as soon as it is no longer deemed necessary.

_____ You agree to report a breach, or anything suspicious that may indicate the potential of a breach to the security of the research data or facilities immediately to the University CISO, even during non-business hours. The current CISO is Matt Langford. He is reachable via office phone at 970-351-1420.

_____ You agree to obtain the approval of the University CISO or an individual designated by the CISO prior to contracting with any vendor who will have access to the research data.

_____ If your research includes the collection of additional data, you have provided a description of the data collection and data transfer method to be used to the University's CISO, and this method had been approved by the CISO or an individual designated by the CISO.

_____ If your research data has been classified as Level 5, the physical configuration and security of your research facility has been approved by the University's CISO or an individual designated by the CISO.

Signature of Research Project Owner: _____ Date_____

Received and Approve by the CISO or designee: _____ Date_____