Contents:

Part 1: Introduction

What is a Data Security and Monitoring Plan?

According to Women's Rights International, a Data Security and Monitoring Plan (DSMP) is "a set of agreed-upon principles and specific practices under which data will be shared without compromising the safety of individuals." Variations on this approach are used in medical and non-medical human subject research, private sector contracts to protect trade secrets, and in large organizations that need to manage sensitive data across many people and platforms.

There are several different terms that describe this type of agreement, for example: data security (&) monitoring plan, data security (&) monitoring protocol, data safety (&) monitoring plan, data safety (&) monitoring protocol, data security agreement, data sharing agreement, and information security policy.

Information contained in this packet

This packet aims to cover two types of information about data security: general usage as well as usage by tribal entities engaged in digital mapping projects.

As far as usage by tribes engaged in mapping, two documents from New Zealand include interesting examples for determining a) the degree of confidentially required by a given data set, and b) qualitative information about undergoing similar GIS mapping projects of sacred sites. These resources can be found in Part 4 of this packet. Examples from the Winnemem Wintu of Northern California (Part 3) and the Coeur d'Alene Tribe (Part 5) are also included.

The general usage examples come from research organizations whose main objective is securing the identity and safety of human research subjects (Parts 6 and 8). Other templates and examples are from a private sector company (Part 7) and a university with diverse IT security needs (Part 9).

The production of the original version of this resource packet was generously funded by the CA Consumer Protection Foundation in 2011. Permission has been granted for reprint of materials contributed by each authoring party of the materials that follow.

For any inquiries and to request DataCenter services in addressing your data security needs in your research project, please contact Jay Donahue, Program Manager, at jay@datacenter.org

Part 2: Creating a Data Security Plan: Questions to Consider

- What is the purpose of this plan?
- What information is covered under this plan?
- What data are deemed confidential?
- Will this confidentiality be rated on a sensitivity scale? If so, how?
- Who will have access to this data?
- How can data be broken into data sets?
- Will different project partners have different levels of access to data sets?
- What are specific procedures for protecting the confidentiality of information?
- Should codes be assigned to data to eliminate identifiers?
- If so, how is the Master Key secured?
- How will confidential data be stored?
- Physical data (posters, etc) v. Digital data (contained in files in mobile devices, servers, etc).
- What are the specific procedures for monitoring the ongoing implementation of this plan?
- What are Adverse Effects of collecting this confidential data?
- If they arise, how will Adverse Effects be noted and addressed?
- Will there be penalties for project participants who don't follow the agreement?
- Will there be a person designated who may impose additional information security requirements beyond those set forth in this policy?
- Will there be an Advisory Board to help with implementation and monitoring?
- What is the process for sharing data with other individuals, groups, or organizations?
- Will there be an expiration date?
- Will there be a timeline for revisiting the plan? If so, Revision History should be included.

****

Part 3: Draft Agreement on Winnemem Wintu Sovereign Control of Maps

This agreement describes how the maps and all data collected and produced during the mapping process will remain under the authority of the Winnemem Wintu Tribe. The agreement covers all mapping that involves [insert list of partner organizations].

Mapping has been used to colonize people, extract resources, and disrupt cultural practices. Mapping has also been used by tribes and communities to advance self-determination, advocate for land rights, build on cultural knowledge and for other beneficial uses. What makes mapping work toward these positive goals depends on who makes decisions about the mapping, who has access to and capacity to use the mapping technology, how the maps are distributed, and other important decisions. This agreement about the Winnemem Wintu mapping is to ensure that the mapping process reflects the Tribe's values and goals.

Collection of Data and Creation of Maps

New map data will be created by using Geographic Positioning Systems (GPS) devices or cell phones with GPS capacity. These devices use signals from satellites to calculate the exact latitude and longitude of a place.

[Insert name(s)] will be able to use the GPS or cell phones to map places. [Insert name(s)] will have full authority in deciding what sites, trails, places are mapped.

Processing and Editing Maps

After the GPS or cell phones are used to create data on the places being mapped, that data will be downloaded to a computer and processed. Processing includes checking that there are not any errors in the data, adding information like place names or location.

[Insert name(s)] will have full authority in deciding who takes the GPS device or cell phone and download the data onto a computer.

[Insert name(s)] will have a computer on which the maps and data can be stored. They are not to be stored on non-Tribe computers. [Insert name(s)] will have full authority to decide which computer can store the data.

[Insert name(s)] will have full authority to decide who will be able to edit the maps on the computer where they are stored.

Sharing the Maps

The maps could potentially be shared within the Tribe and with others through various means, including printed hard copies of maps, map files that can be emailed, and maps uploaded to a website. Different versions of maps can also be created for different groups, such as maps with all data to share with Tribe member and other maps with a selection of some of the data to share with others.

[Insert name(s)] will make decisions about what maps will be shared with who, and what data each of the maps will include.

[Insert name(s)] will authorize sharing of maps with non-Tribe members.

Changes to this Agreement
This agreement may be amended as the mapping process continues and the collected data multiplies, diversifies, and is shared.
[Insert name(s)] will have full authority to make decisions about when this agreement needs to be amended or terminated.
We who have signed below agree that we will not take any action that violates the specifics or the spirit of this agreement.
[Insert list of signatories]

Revision History
[Insert revision dates]

****

Part 4: GIS Mapping of Tribal Lands - Models from New Zealand

A) "Indigenous Values and GIS: a Method and a Framework" by Garth Harmsworth

This article discusses some of the issues that arose during GIS mapping project of Maori sacred sites in New Zealand.

- Source: http://www.landcareresearch.co.nz/science/living/indigenous-knowledge/gis
- Citation: Harmsworth, G.R., 1998: Indigenous values and GIS: A method and framework. Indigenous Knowledge and Development Monitor. Netherlands organisation for international cooperation in higher education (Nuffic). Volume 6, Issue 3, December 1998. Pp 3-7.

"The present research, which made use of participatory methods involving a number of Maori organizations and individuals in New Zealand, established a number of culturally acceptable methods for recording, organizing and making available information on Maori values in a textual and computerized form (Harmsworth 1995, 1997b).

"This produced models linking traditional knowledge— often in both oral and textual form—to GIS and multi-media systems. These models made it possible to store information on Maori values and biophysical information, for the benefit of environmental management planning, while protecting confidentiality and addressing intellectual property rights. Before making use of GIS technology, all information was recorded and organized within a framework (see table 2).

"In the present study, information pertaining to each geographic area was organized and arranged within the framework shown in table 2. The location within the framework indicates the type and special attributes of the knowledge, and determines whether the information may be transferred to more general levels for use by outside agencies. Suitable GIS database structures have been designed to accommodate the setup described above."

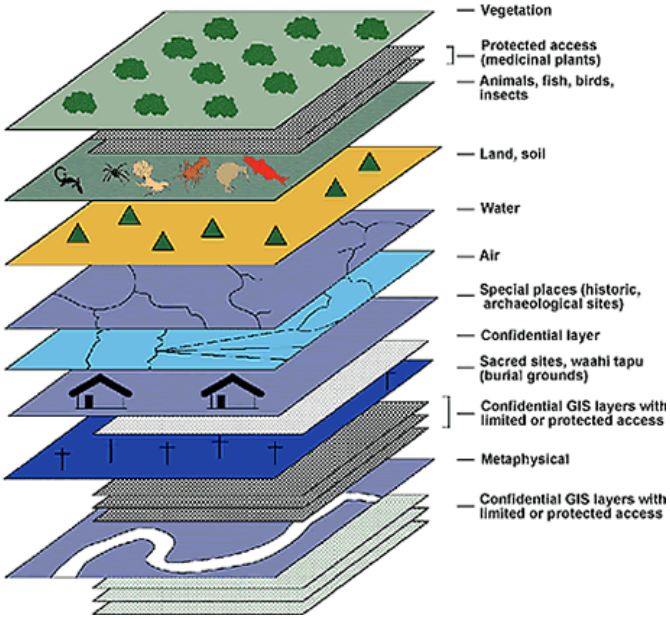
Table 2: A Matrix framework for recording information on Maori Values:

Main groups used in Maori values classification	**a.** National Level, central government (national databases, public domain access)	**b.** Regional and district databases, such as local government (conditions and criteria required for storing confidential information).	**c.** Maori databases such as at the iwi or hapuu tribal level (secured protection of information).	**d.** Individual or group information – extended family (whaanuau) or individual (hihgly sensitive personal information).
1. Vegetation	**1a.** National or regional data on vegetation and land use.	**1b.** Regional or district data on vegetation and land use.	**1c.** Local information on vegetation types.	**1d.** Plant uses, plan varieties, medicinal plants, plants for weaving, etc.
2. Animals, birds, fish, insects	**2a.** National or regional data on animals, birds, etc.	**2b.** Regional or district data on animals, birds, fish, insects.	**2c.** Local information on animals, birds, fish, insects.	**2d.** Special animals, birds, fish insects (such as special foods, cultural harvest, fishing groups, etc).
3. Land, Soil	**3a.** National or regional data on landforms, soils, etc.	**3b.** Regional or district data on landforms, soils, etc.	**3c.** Tribal information on land features, soils, etc.	**3d.** Special landmarks, land features, traditional knowledge on soils and cultivation, muds/ dyes for weaving, etc.
4. Water	**4a.** National or regional data on water.	**4b.** Regional or district data on water.	**4c.** Tribal information on water.	**4d.** Detailed or confidential information on water.
5. Air	**5a.** National or regional data on air.	**5b.** Regional or district data on air.	**5c.** Tribal information on air.	**5d.** Detailed or confidential information on air.
6. Special Places	**6a.** Limited information on special places, cultural sites.	**6b.** Regional and district information on special places, cultural and historic sites.	**6c.** Tribal information on special places, cultural and historic sites (such as archaeological sites).	**6d.** Detailed or confidential information on special places, cultural, and historic sites.
7. Sacred Sites	**7a.** Little or no information at the national or regional level.	**7b.** Regional and district information on some sacred sites (generalized information).	**7c.** Tribal information on sacred sites (such as burial grounds).	**7d.** Detailed or confidential information on sacred sites (such as burial grounds).

8. Metaphysical	**8a.** Little or no information at the national level.	**8b.** No information at the regional or district level.	**8c.** Tribal information on metaphysical information (spiritual, cosmological).	**8d**. Detailed or confidential metaphysical information (such as spiritual, cosmological).

"Once information is stored, links are provided between information at the national level and information accessible at the local or community level; the latter is likely to be detailed and confidential, requiring some form of restricted or protected access. Each piece of information recorded is referenced to an original source or sources, such as a person, book, archive or map, and all references are appropriately coded for database entry.

"Once information is classified and stored in the framework, it can be spatially represented in the form of layers (see figure 1). Each layer is characterized by different levels of detail, sensitivity and confidentiality, which together determine the degree of access at each level."



Knowledge directories
"Information too sensitive or confidential to store in a GIS is linked via a database directory to an individual person. This allows additional information to be obtained from an alternative knowledge source."

Example of options for a Knowledge Directory:

Option	**Example**
(1) Silent or concealed files	Recording the information in an archive or filing system, linked to a GIS database or a map.
(2) Overlay or grid to flag sensitive areas	Recording the information for example as a grid network, which does not identify the actual position or location of confidential or sensitive information such as sacred sites.
(3) Link to books, maps, etc	Setting up a directory to direct the enquirer to associated knowledge in books and maps.
(4) Link to people such as Maori elders.	Setting up a directory to direct an enquirer, via a Maori organization or contact, to and individual for answers to particular questions and associated traditional knowledge.

"Highly sensitive or confidential information can be displayed in the form of a label on a map; alternatively, it can be simply flagged in the GIS as a sensitive or restricted area and the enquirer directed to another information source. This latter option relies on the availability of people with accurate traditional knowledge (Maundu 1995)."

B) "Nga wahi tapu o Ngati Hamua: Sacred sites of Ngati Hamua – Paramount hapu of Rangitane o Wairarapa" by Jason Kerehi, Maori Policy Advisor, Greater Wellington Regional Council

- Source: http://www.gw.govt.nz/document-library-2/category/18
- The section of the paper titled "Challenges and solutions."

Ranking Sites According to Sensitivity

"When the project was first being discussed there was a suggestion that a continuum be developed to establish the level of sensitivity for each site. This measure extended from high sensitivity for those most sacred sites or those sites in areas that were under immediate pressure from development to low sensitivity for sites that were well known and not at risk to development such as a monument in the town park that had protection through the council plan."

This was based on the assumption that "there would be a buffer zone system employed that given the greater sensitivity then a bigger buffer would surround it."

The ranking issue was debated for a long time and eventually it was determined by the researchers that a ranking system was just too hard to quantify for this project. The researchers realized that the issue of ranking was one in which they were not prepared to commit themselves as there were too many variables to consider.

It was agreed to not have a 'buffer zone' i.e. a 50m or 100m exclusion zone. Instead, if a consent activity was anywhere in the vicinity of a recorded site then the iwi were notified. Council staff understood that a recorded site was often part of a larger [pa or community] complex and that it was better to act on the side of caution. The iwi would determine if they needed to enquire further with the landowner.

****

Part 5: Coeur d'Alene Data Sharing Protocol

The following document was created by the Coeur d'Alene in collaboration with several other tribes. It is an interesting document from a tribe that has an extensive GIS program, including a searchable online database. http://www.cdatribe-nsn.gov/IT/InformationTechnology.aspx

Coeur d'Alene Tribe Data License

Agreement made this _____ day of _____, 2010 between the Coeur d'Alene Tribe (hereinafter referred to as Licensor) and the _____ (hereinafter referred to as Licensee).

The Licensor agrees to grant and Licensee agrees to accept nonexclusive and nontransferable license to use the digital data listed below (in accordance with the terms and conditions of this agreement) and referred to in this license agreement as "Data."

Dataset Common Name	File Name

* If additional space is needed please provided in table attached to this document

Licensee hereby accepts such appointment and agrees that all orders for the data placed by the Licensee with Licensor and the relationship of the parties shall be subject to the terms and conditions of this Agreement.

Relationship of Parties

The parties shall be deemed to be solely independent contractors and this Agreement shall not be construed to create any partnership, joint venture, or agency.

Protection of Proprietary Rights
A. The Licensee acknowledges that pursuant to this Agreement it obtains only the right to use the data and that no right, title, or interest in or to any copyrights, trademarks, or other proprietary rights relating to the data is transferred or licensed from Licensor to Licensee.

B. Licensee shall not remove, alter, cover, or obfuscate any acknowledgements, copyright notice, trademark, or other proprietary rights notice placed by Licensor on the data or any portion thereof. Licensee shall comply with directions submitted by Licensor regarding the form and placement of proprietary rights notices on the product, or any portion thereof.
License: Licensor grants a nonexclusive, nontransferable license to the Licensee to use the Data located at the Licensee's address stated above. This license does not grant the Licensee any right to transfer the Data to other parties. If you transfer possession of any copy, modification, or portion of the Data to another party, your license is automatically terminated.

Limited Warranty
The Data is provided "as is" without warranty of any kind. The entire risk as to the results and performance of the Data is assumed by you. Should the Data prove defective, you assume the entire cost of all necessary servicing, repair, or correction. Further, Licensor does not warrant, guarantee, or make any representations regarding the use of, or results from the use of Data in terms of correctness, accuracy, reliability, currentness, or otherwise; and you rely on the Data and results solely at your own risk.

Licensor does warrant, to the Licensee, that the disk on which the Data is recorded is free from defects in materials and workmanship under normal use and service for a period of 90 days from the date of delivery as evidenced by the return to Licensor of the signed and dated original copy of the Product License Agreement. Licensor's entire liability and your exclusive remedy shall be replacement of the disk and/or printed material not meeting Licensor's Limited Warranty and which is returned to the Licensor. If failure of the disk and/or printed material has resulted from accident, abuse, or misapplication of the product, as determined by the Licensor, then Licensor shall have no responsibility to replace the disk and/or printed material under the Limited Warranty.

Terms, Conditions and Termination
This agreement shall become effective on the date Licensor executes the Agreement and transmits an executed copy of the Agreement to the Licensee. The Licensee agrees to provide Licensor with feedback on any errors or modifications that may need to be made to any part(s) of the Data.

This Agreement shall be perpetual and will continue to be in effect until such time as either party terminates this Agreement. Either party may terminate this Agreement with or without cause upon thirty (30) days written notice to the other party. Licensor may terminate this Agreement immediately upon any violation of this Agreement. Upon termination, Licensee shall, if requested by Licensor to do so, return within thirty (30) days the licensed Data. In the event of such termination or in the event of a discontinuation of use of the Data, Licensee will promptly certify in writing to Licensor that the original and all copies in whole or in part of the discontinued or terminated licensed Data have been destroyed.
Returns: Licensee shall return any defective product to Licensor for replacement within ninety (90) days after receipt. Any other returns must be authorized by Licensor.

Amendment and Non-Waiver
This Agreement may not be changed, terminated, or amended without the prior written approval of the Licensor. The Licensee shall be bound by the specifications set forth in the terms and conditions of this Agreement. No course of conduct, action, or inaction on the Licensor's part shall be deemed to be a waiver of any of the Licensor's rights under the Agreement.

Governing Law: This Agreement shall be governed by the laws of the Coeur d'Alene Tribe.

Severability
If any provision of this agreement, or any provision of any document incorporated by reference shall be held invalid, such invalidity shall not affect the other provisions of this Agreement which can be given effect without the invalid provision, and to this end the provisions of this Agreement are declared to be severable.

Part 6: Women's Rights International Data Security and Monitoring Plan

The following document was developed by Shana Swiss, MD, and Peggy Jennings, PhD, of Women's Rights International. It was designed to protect the identities of respondents in a survey about human rights violations in hostile environments. Adapted from data protocols used in biomedical research involving human subjects, this DSMP is meant to be replicated by groups engaged in information gathering that, although non-medical, could have significant negative (and even life threatening) effects on human participants. Source: http://www.womens-rights.org/Documenting/DSMP.html

Women's Rights International:
DATA SECURITY AND MONITORING PLAN: STEPS FOR PROTECTING THE SAFETY OF PARTICIPANTS AND THE SECURITY OF DATA

Local Development Centre; International Women's Human Rights Organisation; and The International Donor Foundation (Example Organizations)

A. PROJECT SUMMARY (EXAMPLE)

The Local Development Centre (LDC), in collaboration with International Women's Human Rights Organisation (IWHRO), and The International Donor Foundation (IDF), are conducting a survey of women who were victims of human rights violations or whose family members were victims of human rights violations. The general topics of the survey are (a) the status of the women's household, education, housing, land, and income before and since the human rights violations, (b) the types of assistance that women sought from government or non-governmental organizations, (c) the types of exploitation and social stigma they may have experienced as a consequence of the human rights violations, and (d) the positive and negative outcomes of specific choices they made with respect to their living situation.

These data will be compiled, analyzed, and presented to the National Commission on Human Rights, and the National Commission on Women's Rights, and the Minister for Women's Health. The findings from this survey will be presented to LDC women's empowerment groups to help them develop advocacy and action plans for changing local laws and practices as well as national laws related to women's access to justice, education, and health care. The findings will also be given to the Women's Media Collective for their series on Women's Health and Human Rights. The goal of presenting these data to these organizations is to advocate for changes in local and national policies and laws that discriminate against women in their ability to gain fair access to justice, to help LDC develop appropriate programs for women affected by human rights violations, and to raise awareness in the community about women and their families who have been affected by human rights violations.

The survey will also give the individual women who participate in the survey and their families the opportunity to learn more about the kinds of community assistance available through LDC . For example, women will have the option of joining the LDC women's empowerment groups, or they may seek assistance from LDC with processes related to access to justice with respect to land rights, health, education, or other aspects of family life that have been affected by the human rights violations.

B. WHAT IS THE PURPOSE OF THIS PLAN? (EXAMPLE)

This plan constitutes an agreement among the individuals associated with the project named in Section A to take every reasonable measure to minimize the potential that someone could be harmed as a result of this survey effort. The most protective measure that we can take is to (a) protect the identity of the women who participate, and (b) protect the confidentiality of sensitive information contained in the survey. This plan indicates how those of us who have access to private or sensitive information will prevent that information from becoming known to others.

The names and addresses of the families on LDC's member list must be protected. Women who have experienced human rights violations are an especially vulnerable group. It is important that the names and addresses of the women who are on the LDC member list and who are selected to participate in the survey are protected very carefully from becoming public.

The answers to the survey items given by specific women must be protected. Some of the questions on the survey contain sensitive information about topics that are considered socially unacceptable or dangerous to discuss . If it became publicly known that a particular woman gave particular answers, she could be at risk for physical, social or other kinds of harm.

C. WHAT INFORMATION IS COVERED UNDER THIS PLAN? (EXAMPLE)

This plan covers all information related to the women's names, addresses, responses to the survey, and the overall findings from the data as a whole. The data sources covered by this plan include the following:

1. LDC Member List: The names and addresses of women on the LDC member list in any form, be it handwritten, printed on paper, or in a computer file format such as Word or Excel.
2. Survey Data Collection Process: The actual interview itself and the completed survey form.
3. Data Entry and Storage: The data entry software and the database file on the computer containing the survey data.
4. Data Analysis: Any computer files or printouts containing data from the survey. This includes data files used for statistical analysis, spreadsheets used for generating charts and graphs, or word processing documents reporting the findings.
5. Findings and Results: Oral presentations and public presentations of the findings or data in any format, including powerpoint files for public presentations. Any other communication of the findings including internet websites, email communications, and any other media of communication.

Additional information can be covered by this plan with the permission of [individual's name], the Director of LDC.

D. WHAT INDIVIDUALS HAVE ACCESS TO THE SURVEY INFORMATION? (EXAMPLE)

The following individuals may have access to some or all of the information covered by this plan, at the final discretion of [individual's name], the Director of LDC:

Local Development Centre: [individual's name], Director of LDC, the LDC research team identified by him, and any LDC staff or associates designated by him. The LDC individuals just mentioned will have access to the following protected data sources and information described in Section C above:

- 1. LDC Member List
- 2. Survey Data Collection Process
- 3. Data Entry and Storage
- 4. Data Analysis
- 5. Findings and Results

International Women's Human Rights Organisation: [individual's name], Director of IWHRO, and [individual's name], Statistical Advisor. The IWHRO individuals just mentioned will have access limited to the following protected data sources and information described in Section C above:

- 3. Data Entry and Storage
- 4. Data Analysis
- 5. Findings and Results

The International Donor Foundation: [individual's name], Program Officer, and [individual's name], Director. The IDF individuals just mentioned will have access limited to the following protected data sources and information described in Section C above:

- 5. Findings and Results

Additional individuals may be added to this plan with the permission of [individual's name], Director of LDC.

E. SPECIFIC PROCEDURES FOR PROTECTING CONFIDENTIALITY OF WOMEN'S IDENTITIES (EXAMPLE)

Each individual named in Section D agrees to keep strictly confidential all information obtained in the course of the survey interviews, contained in the completed survey document, entered into the database, output for data analysis, created to communicate survey findings, and all other information related to the LDC Survey project.

Data or materials that contain names of individuals or other identifying information will not be written on the survey forms nor entered into the survey database. Access to the LDC member list or any other information containing the names or other identifying information about the women who belong to LDC or who participated in the survey will be limited to [individual's name], Director of LDC and the LDC staff he designates.

F. SPECIFIC PROCEDURES FOR PROTECTING CONFIDENTIALITY OF SENSITIVE INFORMATION (EXAMPLE)

Access to survey data and any other information related to the survey is limited to those individuals named in Section D of this document, and may not be discussed, shared, copied, or otherwise transmitted to any other individual, group, or organization without the express written consent of [individual's name], Director of LDC.

Copies of the database files may be copied onto computers or other peripheral devices belonging only to LDC or IWHRO for use within [country] for purposes of data analysis only. Database files may not be carried or transmitted out of [country] without the explicit permission of [individual's name], Director of LDC.
No other use of the data or survey materials is allowed without written consent of [individual's name], Director of LDC.
No original, unique, or source materials or data may be removed from [country]. At the completion of the survey project, all original source materials and data files will be returned to LDC to hold in safekeeping for their own purposes, including storage of backup copies. All other copies of documents and data files in the possession of IDF or IWHRO or otherwise outside of LDC will be destroyed upon completion of the survey project.
No findings or other information about the survey results will be discussed or publicly released without the explicit approval of [individual's name], Director of LDC. He may consult with an Advisory Board to receive input on decisions related to the survey, but the final decision about what to release publicly and what to remain confidential lies with [individual's name], Director of LDC.

G. SPECIFIC PROCEDURES FOR MONITORING THE ONGOING SAFETY OF INDIVIDUALS (EXAMPLE)

[individual's name], Director of LDC, will convene a group of Advisors to assist him in making decisions related to the survey. The main purpose of the Advisory Board is to have a small group of trusted individuals who can assist [individual's name], Director of LDC, to ensure that the best interests of the women continue to be served by the survey effort.

LDC will make every reasonable effort to be aware of any negative experiences that happen to women participants or LDC staff as a result of the survey. If an individual is harmed in some way,[individual's name], Director of LDC, will seek the advice of his Advisory Board to assist him in reviewing the situation to decide whether something about the survey must be modified (or discontinued) to prevent others from experiencing the same kind of negative outcome.
[individual's name], Director of LDC, may also consult his Advisory Board for advice about what aspects of the survey findings should be released publicly and which should be kept confidential.
[End with List of Signatories]

* *

Part 7: SANS Institute Information Sensitivity Policy Template

The following document was developed by SANS Institute, a company that specializes in computer security training and certification for companies, universities, and other organizations. This template is one of SANS Institute's free resources. It assumes the framework of a business entity and reads like a contract between a company and it's employees about how certain information can be accessed, shared, stored, etc.

In contrast to the WRI sample, which was based on the assumption that all data collected through research would be strictly confidential, this template includes guidelines about differentiating between Public and Confidential Information as well as a rubric for creating a Sensitivity Guideline or continuum. Also interesting is guidelines for "marking data." The section on Definitions contains useful information that may help project participants interpret jargon that often populates this types of documents.
Source: http://www.sans.org/security-resources/policies/#template

1.0 Purpose
The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of <Company Name> without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect <Company Name> Confidential information (e.g., <Company Name> Confidential information should not be left unattended in conference rooms).
Please Note: The impact of these guidelines on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to Infosec.

2.0 Scope
All <Company Name> information is categorized into two main classifications:
- <Company Name> Public
- <Company Name> Confidential

<Company Name> Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to <Company Name> Systems, Inc.

<Company Name> Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of our company. Also included in <Company Name> Confidential is information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of <Company Name> Confidential information is "<Company Name> Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to <Company Name> by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into <Company Name>'s network to support our operations.

<Company Name> personnel are encouraged to use common sense judgment in securing <Company Name> Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager

3.0 Policy
The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as <Company Name> Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the <Company Name> Confidential information in question.

3.01 **Minimal Sensitivity:** General corporate information; some personnel and technical information

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential".

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "<Company Name> Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "<Company Name> Proprietary" or similar labels at the discretion of your individual business unit or department. Even if no marking is present, <Company Name> information is presumed to be "<Company Name> Confidential" unless expressly determined to be <Company Name> Public information by a <Company Name> employee with authority to do so.

Access: <Company Name> employees, contractors, people with a business need to know.
Distribution within <Company Name>: Standard interoffice mail, approved electronic mail and electronic file transmission methods.
Distribution outside of <Company Name> internal mail: U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.
Electronic distribution: No restrictions except that it be sent to only approved recipients.
Storage: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.
Disposal/Destruction: Deposit outdated paper information in specially marked disposal bins on <Company Name> premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

3.02 **More Sensitive:** Business, financial, technical, and most personnel information

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". As the sensitivity level of the information increases, you may, in addition or instead of marking the information "<Company Name> Confidential" or "<Company Name> Proprietary", wish to label the information "<Company Name> Internal Use Only" or other similar labels at the discretion of your individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.

Access: <Company Name> employees and non-employees with signed non-disclosure agreements who have a business need to know.
Distribution within <Company Name>: Standard interoffice mail, approved electronic mail and electronic file transmission methods.
Distribution outside of <Company Name> internal mail: Sent via U.S. mail or approved private carriers.
Electronic distribution: No restrictions to approved recipients within <Company Name>, but should be encrypted or sent via a private link to approved recipients outside of <Company Name> premises.
Storage: Individual access controls are highly recommended for electronic information.
Disposal/Destruction: In specially marked disposal bins on <Company Name> premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

3.03 **Most Sensitive:** Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that <Company Name> Confidential information is very sensitive, you may should label the information "<Company Name> Internal: Registered and Restricted", "<Company Name> Eyes Only", "<Company Name> Confidential" or similar labels at the discretion of your individual business unit or department. Once again, this type of <Company Name> Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.

Access: Only those individuals (<Company Name> employees and non-employees) designated with approved access and signed non-disclosure agreements.
Distribution within <Company Name>: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.
Distribution outside of <Company Name> internal mail: Delivered direct; signature required; approved private carriers.
Electronic distribution: No restrictions to approved recipients within <Company Name>, but it is highly recommended that all information be strongly encrypted.
Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.
Disposal/Destruction: Strongly Encouraged: In specially marked disposal bins on <Company Name> premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions
Appropriate measures
To minimize risk to <Company Name> from an outside business connection. <Company Name> computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access <Company Name> corporate information, the amount of information at risk is minimized.
Configuration of <Company Name>-to-other business connections
Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.
Delivered Direct; Signature Required
Do not leave in interoffice mail slot, call the mail room for special pick-up of mail.
Approved Electronic File Transmission Methods
Includes supported FTP clients and Web browsers.
Envelopes Stamped Confidential
You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.
Approved Electronic Mail
Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, [insert corporate supported mailers here…]. If you have a business need to use other mailers contact the appropriate support organization.
Approved Encrypted email and files
Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within <Company Name> is done via a license. Please contact the appropriate support organization if you require a license.
Company Information System Resources
Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.
Expunge
To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data, supplied as a part of Norton Utilities. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten. The same thing happens on UNIX machines, but data is much more difficult to retrieve on UNIX systems.
Individual Access Controls

Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On Mac's and PC's, this includes using passwords on screensavers.

Insecure Internet Links

Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of <Company Name>.

Encryption

Secure <Company Name> Sensitive information in accordance with the *Acceptable Encryption Policy*. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

One Time Password Authentication

One Time Password Authentication on Internet connections is accomplished by using a one time password token to connect to <Company Name>'s internal network over the Internet. Contact your support organization for more information on how to set this up.

Physical Security

Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Private Link

A Private Link is an electronic communications path that <Company Name> has control over it's entire distance. For example, all <Company Name> networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer have established a private link. ISDN lines to employee's homes is a private link. <Company Name> also has established private links to other companies, so that all email correspondence can be sent in a more secure manner. Companies which <Company Name> has established private links include all announced acquisitions and some short-term temporary links

Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu

* *

Part 8: Template - University of North Texas Health, Protocol Synopsis for Research Involving Materials That Have Already Been Collected

The following protocol comes from the Institutional Review Board at the University of North Texas' Office for the Protection of Human Subjects. It uses a series of questions to guide researchers through the process of writing data protocol. It is likely that this document is used in biomedical research involving human subjects, particularly in situations where research is being transferred from one research entity to another. Some irrelevant content has been omitted. Nevertheless, it contains some key points that the tribe may want to consider, and the 'question and answer' format may be especially adaptable for a participatory drafting process among tribal leaders and members.

This template contains the first mentions of "stripping the data of identifiers" – a process of encryption that transforms recognizable data into coded language. Each sacred site could be given a number, for example, with only members of the tribe knowing what name and context that number represents. The guidelines for making a Risk Assessment for the data may be especially helpful for conceptualizing what needs to be included in the data security plan.

Source: http://www.hsc.unt.edu/sites/OPHS-IRB/index.cfm?pageName=Instructional Guidelines

Protocol Information

***Title of Project*:**

Name of Principal Investigator:

Name of Co-Investigator (s):

Sponsoring Agency/Company (if applicable):
Sponsor's Protocol Number (if applicable):

Purpose of the Study- *State the scientific objectives of the research.*

Background and Significance – *Briefly sketch the background leading to the present proposal.*

Preliminary Studies- *Summarize preliminary studies conducted by the investigator pertinent to this proposal. State "none" if applicable.*

Description of Associated Research Projects
1. Description of the parent project-*Describe the original project from which the data originated from, including where the data is currently stored.*

Description of THe samples and Behavioral/health data that will be used in this study
1. Description of the data-*Describe the data that will be analyzed in this study, including the source of the data (survey/questionnaire, medical record, research record, etc), the type of health information present, the format of the data (i.e. electronic or hard copy), and how the data will be labeled.*

2. Describe any identifiers that will be present in the data when it is received by UNTHSC researchers.

3. When appropriate, describe the process for "stripping" the data of identifiers-*Describe where and when this will occur, who will perform the stripping process, where the master list will be maintained (if appropriate), what identifiers will remain after this process, and who will have access to the identifiable information.*

Transfer of the Samples and Related Data
1. Transfer in of data to UNTHSC from outside researchers. *In this section, describe the process for how the data will be transferred to UNTHSC. List the name of the organization(s) they will be received from, and the person (s) at that organization (s) responsible for overseeing the transfer of the samples to UNTHSC. If the data will be received from more than one entity, please describe appropriately.*

2. Transfer out of the data from UNTHSC to outside researchers: *In this section, describe the process for how the data will be transferred from UNTHSC to outside organizations or individuals. List the name of the organization (s) and individuals they will be sent to, and the person(s) who will be responsible for receiving the samples and data at that organization.*

3. Transfer of the related data internally (to/from other UNTHSC researchers)-*In this section, describe the process for how the data will be transferred from or to other investigators at UNTHSC. Note-IRB review and approval of the investigator's research project to which the data will transferred to is required before the transfer can occur.*

Analysis of the data
1. Setting/Location-*Describe where the data will be analyzed (i.e. UNTHSC or outside entity).*

2. Procedures for Data Analysis-*Describe where the data analysis will occur, plans for statistical analysis of data when appropriate, and key personnel that will be involved.*

3. Estimated Period of Time to Complete the Study-*Describe the stages and overall time for the data analysis (start to completion).*

Storage of the data
1. Short term storage of the data -*Describe where the data (electronic and hard copy) will be stored when it is received by UNTHSC researchers and during analysis.*

2. Long term storage of the data-*Describe where the data will be stored after this project is completed. If appropriate, describe when the data will be destroyed.*

RISK/BENEFIT assessment
1. Potential Risks- *Describe any **informational risks** (including breach of privacy, confidentiality risk, document access, risk of embarrassment, and other "risks" related to how sensitive information is stored, accessed, and managed) as well as any **procedural risks** (risks associated with the actual process or procedures associated with the study) to the human subjects whose data will be used for this project.*

2. Potential Benefits- *Describe any potential benefits to the human subjects, society and/or science that may result from this research project.*

3. Risk/Benefit Assessment –*Describe how the anticipated benefit of the research justifies the risk to the human subjects whose data will be used for this project.*

Special precautions-
1. Data Storage and Security- *Describe how the data will be secured during storage. The investigator must take necessary steps to maintain confidentiality of the data. This includes coding data and choosing an appropriate and secure data storage mechanism which will prevent unauthorized access to the data. State who will have access to the data. If data with subject identifiers will be released, specify the person(s) or agency to whom the information will be related and the purpose of the release.*

2. Ensuring the data is legally and ethically obtained-*Describe how it was verified that the data that will be used in this study was obtained legally and ethically. This may be demonstrated by obtaining a copy of the IRB approval for the collection of the data from the outside entity, as well as a clinical consent document or research consent form indicating that the subjects gave their permission for the data to be used for research purposes. A copy of this documentation should be submitted with the IRB Application.*

Ownership of DATA- *Describe what individual/entity will own the data after it is transferred to UNTHSC. Indicate if the outside entity will retain any ownership, or access to the data, after transfer.*

Key personnel- *List all individuals directly involved in the conduct, design, or reporting of research involving human subjects in the study, and describe their role.*

LITERATURE CITED- *If any, the references should be limited to relevant and current literature pertinent to the proposed research.*

* *

Part 9: George Washington University Information Security Policy

The following document is used by George Washington University to outline a data security agreement among faculty, staff, and students to maintain the security and confidentiality of the University's computer networks and data communications infrastructure.

Unlike Samples 1 - 3, this is not a template. It is also different because it takes the form of an agreement that parties involved in the project could sign. Included it in this packet because the overall outline may be appropriate and the sections on Securing Information on Workstations may be useful for mapping projects. Source: http://my.gwu.edu/files/policies/InformationSecurityPolicyFINAL.pdf

INFORMATION SECURITY POLICY

1. Policy Statement

Maintaining the security, confidentiality, integrity, and availability of information stored in the University's computer networks and data communications infrastructure ("University systems") is a responsibility shared by all users of those systems. All users of University systems are responsible for protecting those resources and the information processed, stored or transmitted thereby as set forth in this policy. Violations of this policy may result in disciplinary action up to and including termination or expulsion.

Reason for Policy/Purpose: Information is a vital University asset and requires protection from unauthorized access, modification, disclosure or destruction. This policy sets forth requirements for incorporation of information security practices into daily usage of University systems.

Who Needs to Know This Policy: Faculty, staff and students

Policy/Procedures: Users of University systems are responsible for protecting the information processed, stored or transmitted over or on those systems, and for incorporating the following practices into their daily activities.

A. Maintaining the Integrity of Information

The soundness and completeness of information on University systems must be maintained during its transmission, storage, generation, and/or handling. Information that is corrupted or modified may be impossible to use or lead to errors in decision-making. To maximize the integrity of data, information technology (IT) computing resource users shall adhere to the following:

1) Screen all non-text files downloaded from the Internet with anti-virus software prior to usage to minimize the risk of corruption, modification or loss of data.
2) Notify the Chief Security Officer in the Division of Information Technology (IT) immediately if passwords or other system access control mechanisms are lost, stolen or disclosed, or are suspected of being lost, stolen or disclosed.
3) Forward information pertaining to security-related problems to the Chief Security Officer immediately. DO NOT further distribute this information.
4) Use information obtained from the Internet with caution. Before using free Internet-supplied information for business decision-making purposes, corroborate and confirm the information by consulting other reliable sources.

B. Protecting Confidential Information

All members of the University community are obligated to respect and protect confidential data, and to follow the Data Classification Security Policy. The University strongly discourages storage of any confidential or sensitive data on any computer or network-attached device that has not been explicitly approved by personnel from the Information Security Office within the Division of IT. IT computing resource users must adhere to the following:

1) Employ adequate encryption technology for sensitive or critical information such as educational records, Social Security Numbers, identification numbers (GWID), and credit card numbers in accordance with the Mobile Device Security Policy. For specific information regarding encryption technology options, e-mail the Division of IT at infosec@gwu.edu.
2) Notify the Chief Security Officer at abuse@gwu.edu if sensitive or critical University information is lost or disclosed to unauthorized parties, if any unauthorized use of University systems has taken place, or if there is suspicion of such loss, disclosure or unauthorized use.
3) DO NOT post University material such as software, internal memos, or other non-public information on any publicly-accessible computer or website unless first approved by the appropriate authority.
4) DO NOT store Confidential Data in any computer unless the persons who have access to that computer have a legitimate need-to-know the information involved.
5) DO NOT save fixed passwords in web browsers or e-mail clients when using a University system. This may allow unauthorized users to access critical or sensitive information such as that contained in Banner, the Enterprise Accounting System or the Advancement System.
6) DO NOT distribute critical or sensitive University communications to external entities. Only distribute to internal entities on a need to know basis.
7) DO NOT establish Internet or other external network connections that could allow non-University users to gain access to University systems with critical or sensitive information unless prior approval has been received from the appropriate authority.
8) DO NOT discuss information security-related incidents with individuals outside of the University, or with those inside the University who do not have a need-to-know.

C. Utilizing Strong Passwords
Passwords are an integral part of overall security. To minimize the risk of a password being compromised and data being lost due to unauthorized access, follow the guidance in Password Do's and Don'ts.

D. Securing Information on Workstations
Users of University systems must adhere to the following procedures to minimize the potential for theft, misuse, or corruption of data:

1) Always use a security cable or locking device with laptop computers and secure mobile devices in accordance with the Laptop Computer and Small Electronic Device Theft Policy, particularly when away from their office or work space.
2) Secure personal computers by requiring a password when the computer is turned on and when the screen saver is deactivated (public computers with no critical or sensitive information, such as those in the library or in labs, are excluded).
3) Log out of the system when finished working.
4) Use secure means to transmit confidential data. Email is not a secure means to deliver information. Information that is sent by email is at risk. Avoid using e-mail to transmit confidential data.
5) Keep all computer software up to date with the latest software maintenance releases. [omitted text]

E. Who Approved This Policy
F. History/Revision Dates: Origination Date, Last Amended Date, Next Review Date

****

Revised edition October 2012
By Mara Ortenburger, DataCenter
datacenter@datacenter.org

About the DataCenter: *DataCenter supports community-led organizations to use research and documentation as a tool to unleash the power of their expert knowledge, and effectively shape their lives and futures. Our approach involves making information accessible, transferring research skills, supporting community-led documentation, and legitimizing community knowledge in institutional decision-making that impact their lives and communities. We believe a just and sustainable future will emerge from community that has control over, access to, and capacity to produce and apply their rich knowledge to protect and advance community interests.*

Franklin Street, Suite 900, Oakland, CA 94612
(510) 835-4692 ▪ datacenter@datacenter.org