**Guidelines for the Use of Sync.com Service for Research Involving Humans**

Faculty and student research and teaching activities involving the use of human participants, (using human subjects, human tissue, human stem cells or data collected on human subjects) under the auspices of UNBC must conform to the UNBC Policy on Research Involving Human Participants and must have the prior approval of the UNBC Research Ethics Board.

Before any personal information pertaining to research as defined above can be managed using Sync.com, please ensure a UNBC Research Ethics Board review has approved the use of Sync.com for your research project. Using Sync.com for research to manage Confidential or Restricted information as defined below requires UNBC Research Ethics Board review and approval. Visit the Research Ethics webpage to download the [current application form](http://www.unbc.ca/research/forms#Research%20Ethics%20Humans) for review, and contact the Research Ethics Officer if additional information is needed.

If you have already been approved by the Research Ethics Board to use the UNBC FilePortal for secure file transfer of identifiable information before it was decommissioned, you may use Sync.com under the same conditions that you were approved to use FilePortal ensuring that Sync.com is used to only transfer data, and not for data storage.

If personal information is managed using Sync.com without a Research Ethics Board review because the review is not required, or because of negligence, the individual using Sync.com without approval assumes total personal responsibility for the management of the information using the Sync.com service.

Before starting to use Sync.com for secure data transfer, consider what type of information you are managing by reviewing the categories below. The objective of a research study may make any listing of information sensitive, thus the research ethics protocol for data security that was approved by the UNBC Research Ethics Board is to be followed in all instances.

**Public Information and Data – Minimal Risk and/or Minimal Impact**

**Description:** This is factual information that a reasonable person would feel comfortable posting on a public facing webpage or posting in a public forum. Examples include business contact information and any information that is freely available, such as published research, published marketing materials, public event information and public announcements. This data will not contain any personally identifiable information unless the individual has provided written informed consent that the information can be released to the public.

**Storage:** This type of information can be collected, stored, and disposed of at the user’s discretion, with minimal security measures taken. This information can be stored on unencrypted drives and used on public or office devices.

**Sharing:** This information can be freely shared to respond to routine requests.

**Internal - Low Risk and/or Low Impact**

**Description:** Internal data may contain personal information. When personal information is present, the personal information will not be structured to precisely or easily reveal sensitive information about an identifiable person. Personal information if intentionally or unintentionally released would cause a low level of damage to the individual identified. Data may include budgets, advice, recommendations, work schedules, vacation calendars, draft administrative materials and other material that requires approval to be released to the public, but does not meet the criteria of Confidential or Restricted.

**Storage:** Standard internal information will be stored on devices and drives that are encrypted and password protected. This information and data will be stored on Canadian servers that do not backup information to another country.

**Sharing:** Standard internal information will be shared only with authorized users. If you are unsure if sharing this information is covered in your Research Ethics Board approval, contact the Research Ethics Officer or I.T. Security.

**Confidential – Moderate Risk and/or Moderate Impact**

**Description:** This information contains personally identifiable information or aggregated personal health information containing elements that have a low risk of re-identifying individuals. Spreadsheets, databases, or unstructured data revealing standard customer, employee, student or client information with individual identifiers are examples of confidential records.

**Storage:** This information will be stored on devices and drives that are encrypted and password protected. This information will only be stored in locations approved by your Research Ethics Board.

**Sharing:** This information will be shared only with users approved by the Research Ethics Board. Information will be stored in a password protected folder and access only granted to authorized users.

**Restricted – High Risk and/or High Impact**

**Description:** Personally identifiable information that can be combined to perform identity theft or create an invasive profile of an individual. Data may include unstructured or structured personal health records identifying an individual. Personal information banks or compiled documents that contain the following information must be classified as restricted information.

* Birth certificate information/photocopies
* Social insurance numbers/photocopies
* Driver’s license numbers/photocopies
* Medical service card numbers/photocopies
* BC ID numbers/photocopies
* Passport numbers/photocopies
* Student/work permit information/photocopies
* Temporary resident visa information/photocopies
* Excerpts from/copies of an individual’s medical files/history

**Storage:** This data must be stored on university drives or devices approved by your Research Ethics Board. Data and information in this classification must be stored on encrypted and password protected devices and drives and must be stored in a password protected folder or password protected archive file. Contact the IT Security Analyst for instructions to properly secure archive and zip files.

**Sharing:** This data will not be shared unless authorized by the Research Ethics Board. Passwords will not be transmitted in plain text and will be sent in separate communication from links to the files or folders. The safest method would be to call the recipient and provide the password to the encrypted file over the phone.

**Purging documents from Sync.com**

Once a record stored on Sync no longer requires a legal or operational copy to be stored there, that record needs to be removed from Sync by purging the record. Follow the “Instructions on disposing documents from Sync.com” process document to purge documents from Sync.com

**Support and Inquiries**

Each employee is responsible for the management of UNBC records. The university community can support you in managing that responsibility. If you are experience technical difficulties with the Sync.com service, use the Sync.com FAQs, Sync.com official user manual and contact Sync.com technical support. If you have any questions regarding data security or research ethics that are not covered in these guidelines, feel free to contact:

***Data Security Inquiries***

Annette Doyle

IT Security Analyst

250-960-6324 (26324)

Annette.doyle@unbc.ca

***Research Ethics Inquiries***

Isobel Hartley

Research Ethics Officer

250-960-6735 (26735)

Isobel.hartley@unbc.ca