Canadian Cooperative Wildlife Health Centre
Data Security Policy

1. Effective Date: September, 2007

2. Purpose

To ensure conformity with Federal/Provincial/Territorial privacy legislation, specifically to ensure that personal information is being stored properly and securely in accordance with laws and policies dealing with the collection, use, disclosure and retention of personal information.

To ensure that CCWHC practices and polices are in accordance with federal policies and guidelines pertaining to contractual security, including information technology security provisions.

To assure sponsoring agencies and the public that the CCWHC is responsible with establishing and maintaining standards of care that are in conformity with government and University policies and Federal/Provincial/Territorial legislation.

To ensure that proper consideration is given to CCWHC contractual obligations and processes, including conformity with Public Works and Government Services (PWGSC) Industrial Security Directorate and Security and Contract Management provisions.

To establish the responsibilities of the CCWHC Privacy coordinator/Chief Information Officer and the IT Security Coordinator the establishment of which are necessary requirements within Treasury Board of Canada and PWGSC contracting guidelines as well as a requirement under the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

3. Scope and Application

This policy has been developed in the context of, and is designed to complement the *CCWHC Privacy Policy*, the *CCWHC IT and Data Use Agreement*, the *CCWHC Privacy Policy and Data Use Agreement Guidelines*, and the *CCWHC Data Sharing/Confidentiality Policy*. In addition it is designed to compliment existing University policies and regulations, particularly those governing computer use and data management. Additional policy consideration was given to federal government policies pertaining to data security, privacy, and data management, specifically those derived from the Treasury Board of Canada, Public Works and Government Services Canada, and the Office of the Privacy Commissioner of Canada.

Particular attention was given to the PWGSC Industrial Security Directorate and Security and Contract Management provisions. Public Works and Government Services Canada – Industrial Security Directorate is responsible for developing policy guidelines pertaining to security and contract management for many federal government agencies, including

the Canadian Food Inspection Agency, the Public Health Agency of Canada and the Department of Fisheries and Oceans. In some instances PWGSC is responsible for the provision of contracts on behalf of these agencies as well. An increasingly frequent contractual requirement is the need to qualify for basic security clearances, both individual and/or institutional. In order to be eligible for these contracts you must apply and receive the requisite security clearance, in order to receive the clearance you must demonstrate conformity with the necessary guidelines, one of which is the creation of a data security policy, this policy is a proactive response to this issue. Establishment of a Privacy coordinator/CIO and an IT security coordinator are also necessary requirements to conform with these guidelines and contractual requirements.

4. Definitions

Information Technology Security - The *Government Security Policy* defines IT security as the "safeguards to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information."

5. Policy

Information systems must be secured against rapidly evolving threats that have the potential to impact their confidentiality, integrity, availability, intended use and value. This dictates that the CCWHC apply baseline security controls, continuously monitor service delivery levels, track and analyze threats to CCWHC IT systems, and establish effective incident response and IT continuity mechanisms.

Effective security of information requires a systematic approach that identifies and categorizes information and associated assets, assesses risks to them, and implements appropriate personnel, physical, and IT safeguards

Access to CCWHC data is granted internally when a legitimate need for the data is demonstrated, and externally when release of such data would not violate CCWHC stewardship obligations, privacy legislation, or legal contracts, for more information on data sharing please see the *CCWHC Data Sharing/Confidentiality Policy*

5.1 Roles and Responsibilities

Various pieces of legislation, including *PIPEDA* and the *Privacy Act*, as well as several federal government policies, specifically those pertaining to data security and privacy involving the Treasury Board of Canada, PWGSC and the office of the Privacy Commissioner of Canada propound that an organization is responsible for personal information under its control. A requirement for the effective management of this data is the need to designate an individual or individuals who are accountable for the organization's compliance with applicable legislation and policies i.e. the establishment of an Information Technology Security Coordinator and the establishment of a Privacy Coordinator/Chief Information Officer (in the case of the CCWHC this would be the

Director of Information Technology and the Director of Policy, Finance and Administration, respectively).

IT Security Coordinator
The IT Security Coordinator is responsible for:

- The development and implementation of IT security procedures
- The assessment of security threats to CCWHC data
- The monitoring and recording/reporting of security incidents
- Ensuring IT operational personnel are aware of and in conformity with this and other data security policies
- The overall security of the system including system hardware and software
- The review and revision of the IT security procedures and the review of supporting documentation, including the Data Security Policy
- Determining retention periods for essential business information and archived backups

Chief Information Officer/Privacy Coordinator
The Chief Information Officer is responsible for:

- Ensuring the effective and efficient management of the department's information assets, this includes the duty to ensure that users are knowledgeable about and in compliance with federal and provincial privacy legislation
- The creation of policies exemplifying conformity with legislation and guidelines relating to data sharing, privacy and confidentiality requirements
- Assuring conformity between CCWHC practices, government legislation and polices and CCWHC contractual agreements
- Ensuring compliance with PWGSC Security and Contracting Management Standards
- Establishing written security arrangement and/or confidentiality agreements that defines the terms and conditions of any authorized sharing, and recognize any legal impediments to the sharing in appropriate circumstances
- The review and revision of all CCWHC policies, including the Data Security Policy and for recommending the review and revision of IT security procedures
- Determining retention periods for essential business information and archived backups

IT Operational Personnel
It is the responsibility of IT operational personnel to:

- follow security procedures and recommend improvements to them,
- respond to security incidents,
- test and install security patches,
- maintain or upgrade security hardware and software,
- monitor systems and logs,

- back up and recover information
- manage access privileges and rights
- test backups regularly to ensure that they can be used for recovery
- back up all software and configuration data
- facilitate the restoration of data and services
- test restoration procedures regularly to ensure that they are effective and that they can be completed within the time allotted for recovery

Ultimately, the secure storage of CCWHC data is a joint responsibility of system administrators, database designers, application designers, and the data user who must ensure that passwords and other security mechanisms are used.

5.2 Policy Requirements

The CCWHC must conduct an annual assessment of the IT security program and practices to monitor compliance with government and university security policies and standards. The IT security coordinator and privacy coordinator must inform and regularly remind personnel of IT security responsibilities, concerns and issues.

In the event of a possible security incident, documented response procedures must outline how Help Desk personnel will document the event, identify trends, notify the IT Security Coordinator and instruct the user on how to proceed.

The CCWHC must ensure the incorporation of identification and authentication safeguards in all networks and systems, according to the level or risk for the network or system. When assigning a unique identifier for users, CCWHC IT personnel must ensure the proper identification of the individual to whom the identifier is issued. This entails that IT and information access be restricted to individuals who have been screened and authorized. The mechanism to ensure this screening is already in place with the CCWHC Data Use Agreement Application Form, which requires each application be authorized by a non-term CCWHC representative. The level of access granted must be kept to the minimum required for individuals to perform their duties (i.e., the least-privilege principle).

The CCWHC shall withdraw access privileges from individuals (including students, contractors, or others) who leave their current organization, and revise access privileges when individuals move to jobs that don't require the same level of access. A renewal period of one year has been implemented in the CCWHC Data Use Agreement, except in the case of CCWHC representatives, specifically the user agreement states that “all accounts, except those of non-term CCWHC representatives, will expire within one year from the date of establishment or at the closing of the designated period of employment indicated on the account application form. In all circumstances, except that mentioned above, the duration of the account will not be for a period of greater than one year.”

6. References

Legislation (and accompanying regulations)

Local Authority Freedom of Information and Protection of Privacy Act
Freedom of Information and Protection of Privacy Act
Access to Information and Protection of Privacy Act
Personal Information Protection and Electronic Documents Act
Privacy Act
Access to Information Act

Related Policies

CCWHC Privacy Policy
CCWHC Information Technology and Data Use Agreement
CCWHC Data Sharing/Confidentiality Policy
CCWHC Privacy Policy and Data Use Agreement Guidelines
Government Security Policy (Treasury Board of Canada)
Policy on Management of Information Technology (Treasury Board of Canada)
Privacy and Data Protection (Treasury Board of Canada)
Policy on Information Management (Treasury Board of Canada)
Policy Framework for Information and Technology (Treasury Board of Canada)
Operational Security Standard: Management of Information Technology Security (PWGSC)
Security and Contracting Management (PWGSC)
Security Organization and Administration (PWGSC)
Industrial Security Manual (PWGSC)
University of Guelph Protection of Privacy and Access to Information Policy
University of Saskatchewan Policies - Data Management, Data Access and Data Use
University of Saskatchewan Policies-Network Security
University of Saskatchewan Policies-Computer Use

7. Contact

CCWHC Director of Policy, Finance and Administration (privacy coordinator/chief information officer), phone 306.966.6060

Director of IT Services (IT Security Coordinator), phone 306.966.5162