UNIVERSITY OF MANITOBA

UNIVERSITY OF MANITOBA
PROCEDURE

Procedure:	**CUSTODY AND CONTROL OF ELECTRONIC DEVICES AND MEDIA PROCEDURES**
Parent Policy:	Custody and Control of Electronic Devices and Media Policy
Effective Date:	June 23, 2015
Revised Date:	
Review Date:	June 23, 2025
Approving Body:	Vice-President (Administration)
Authority:	
Responsible Executive Officer:	Vice President (Administration)
Delegate: (if applicable)	Chief Information Officer, IST
Contact:	IT Security Coordinator
Application:	All employees

Part I
Reason for Procedure

1.1 To set out procedures secondary to the policy entitled "Custody and Control of Electronic Devices and Media Policy" with respect to the removal or destruction of Data on Electronic Devices or Media when redeploying, recycling, repairing offsite, returning to a vendor or otherwise removing an Electronic Device or Media temporarily or permanently from University property and stewardship.

Part II
Procedural Content

These Procedures are to be read in conjunction with the Custody and Control of Electronic Devices and Media Policy and all capitalized terms used herein shall have the meaning given to them in the Policy.

Shared Use Devices

2.1 Wherever practical, there should be clear ownership of Data that is stored on Electronic Devices and Electronic Media; in other words, there should be evidence which individual has control and custody of information contained on a given Electronic Device or Electronic Media.

2.2 In circumstances where there is shared use of an Electronic Device or Electronic Media, the responsible technical representative shall determine the methods that will be used to maintain the custody, control, and security of information stored on the Electronic Devices or Media. These methods might include, but are not limited to, encryption, segregation and securing of user profiles and data, and use of secure network storage.

2.3 When changes occur in the membership of the group of people that have shared use of an Electronic Device or Electronic Media, the responsible technical representative will determine whether the change in membership constitutes a change in custody and control (of the Electronic Device or Electronic Media) and whether the change presents a material increase in risk due to the potential to access information. In the cases where the shared use Electronic Device or Electronic or Media remains in the custody and control of the remaining group members, normally, there would not be a requirement to wipe or destroy all Data on the Electronic Device or Electronic Media; however, it may be appropriate to wipe or destroy data that was stored in profile that was uniquely associated with a person who has left the user group. For example, if there is shared use of a personal computer in a laboratory and one of the users ceases to work in the laboratory then it would be appropriate to delete that user's profile and selectively wipe all data uniquely associated with that profile. The nature of the information and, correspondingly, the level of involved risk, shall be considered in the evaluation of shared use situations. If the technical representative is unsure as to the appropriate approach or method for a given situation then they should consult with the IT Security Coordinator.

Record Keeping

2.4 Records shall be kept of the destruction of Data contained on Electronic Devices and Electronic Media. At a minimum, these records shall include the following information:

(a) The date on which the Data was destroyed;

(b) The name of the person who owned or was responsible for the Data (i.e. had custody and control of the Data) prior to its destruction;

(c) The name of the technical representative responsible for providing technical support related to the Electronic Device or Electronic Media;

(d) The chain of custody of the Electronic Device or Electronic Media from the owner/user of the equipment through the destruction of the Data; and

(e) Any other information that is required to be recorded by another applicable policy or procedure (e.g. approval to dispose of an asset).

Grace Period

2.5 A Custodian shall be granted a Grace period of a minimum of ten (10) business days between forfeiture of custody and control of the Electronic Device and Electronic Media and destruction of the Data on the Electronic Device or Electronic Media. The purpose of this Grace Period is to allow the Custodian an opportunity to verify that they have functional copies or archives of any data that they want to retain.

2.6 The technical representative responsible for supporting the Electronic Device or Electronic Media from which Data will be destroyed is responsible for informing the Custodian of the Grace Period and of the fact that the data on the Electronic Device or Electronic Media will be permanently destroyed after the conclusion of the Grace Period.

Custody and Control of Devices and Media Pending Data Destruction

2.7 During the period that commences with the Custodian forfeiting control of the Electronic Device or Electronic Media and ends with the destruction of the Data, the Electronic Device or Media shall be transported and stored in a secure manner. Physical access to the Electronic Device and Electronic Media shall be restricted to only those persons who are authorized to carry out the decommissioning process and to transport and store the Electronic Devices or Electronic Media. Persons responsible for the decommissioning process will not normally be provided access to the data on the Electronic Device or Media that they would not normally have; i.e. Custodians should not normally provide passwords used to access Data on Electronic Devices to persons responsible for the decommissioning process.

2.8 Electronic Devices and Electronic Media that might contain sensitive or confidential information may be transported intra-campus (i.e. routes that are contained within University property) by either the responsible Technical Support Representative or by the Truck Messenger service provided by Physical Plant.

2.9 Technical Support Representatives are responsible for assessing whether a given Electronic Device or Electronic Media might contain sensitive or confidential information. Physical Plant will accept requests to transport Electronic Devices and Electronic Media that might contain sensitive or confidential information only when the request originates from the Help and Solutions Centre. Technical Support Representatives must work through the

Help and Solutions Centre to arrange transportation of Electronic Devices and Electronic Media that might contain sensitive or confidential information.

2.10 Requests for transportation of Electronic Devices or Electronic Media that might contain sensitive information must be made to Physical Plant by a representative of the Help and Solutions Centre. The Help and Solutions Centre will provide Physical Plant with an IT service management ticket number (e.g. a Cherwell ticket). Physical Plant will only pick up equipment that has been tagged with the corresponding ticket number.

2.11 Technical Support Representatives may request transportation of Electronic Devices and Electronic Media by Physical Plant directly to an (external) collector of electronic waste only when the Technical Support Representative has determined that that Electronic Devices and/or Electronic Media do not contain sensitive information, either because of the use profile of the Electronic Device or Electronic Media or because appropriate steps have been taken to remove or destroy Data that was contained on the Electronic Devices or Electronic Media.

2.12 If Electronic Devices or Electronic Media might contain sensitive or confidential information and they must be transported inter-campus or to/from an off-campus location (i.e. if the transportation route involves traversing off-campus property) then the Data on the Electronic Devices or Electronic Media must be encrypted, destroyed, or removed before the equipment is transported.

Data Destruction

2.13 Whenever possible, Electronic Media or Electronic Devices that have been deemed to be electronic waste (and is destined for recycling or disposal) shall be physically destroyed by crushing or shredding the Electronic Media and/or Electronic Device using the service provided by the Help and Solution Centre and following the guidelines contained in the Data Destruction Standard. Procedures for Data Destruction are covered in Part A of the Data Destruction Standard.

2.14 Electronic Media or Electronic Devices transferred within the University (e.g. reassigned from one employee to another employee), donated to an outside organization, or returned to a vendor at the end of a lease must have data removed according to industry best practices for Clear (minimum) or Purge (preferred). If Electronic Media or Electronic Devices are leaving the property or stewardship of the University for repair or transport, Data should be securely encrypted whenever possible and appropriate agreements must be in place with external parties to ensure that the Data is handled and protected appropriately.

2.15 In the event of a non-functioning Electronic Device or Electronic Media going out for repair, or if it is undesirable or impossible to remove data before sending for repair, contact the IT Security Coordinator for guidance.

2.16 Procedures which persons responsible for wiping of data from various types of Electronic Devices and Electronic Media must follow are covered in Part B of the Data Destruction Standard.

Part III
Accountability

3.1 The Office of Legal Counsel is responsible for advising the Chief Information Officer, IST that a formal review of this Procedure is required.

3.2 The Chief Information Officer, IST is responsible for the implementation, administration and review of this Procedure.

3.3 All employees are responsible for complying with this Procedure.

Part IV
Review

4.1 Governing Document reviews shall be conducted every ten (10) years. The next scheduled review date for this Procedure is June 23, 2025.

4.2 In the interim, this Procedure may be revised or repealed if:

(a) the Chief Information Officer, IST or Approving Body deems it necessary or desirable to do so;

(b) the Procedure is no longer legislatively or statutorily compliant;

(c) the Procedure is now in conflict with another Governing Document; and/or

(d) the Parent Policy is revised or repealed.

Part V
Effect on Previous Statements

5.1 This Procedure supersedes all of the following:

(a) all previous Board of Governors/Senate Governing Documents on the subject matter contained herein; and

(b) all previous Administration Governing Documents on the subject matter contained herein.

Part VI
Cross References

6.1 This Procedure should be cross referenced to the following relevant Governing Documents, legislation and/or forms:

(a) Processes and Procedures for Commissioning and Decommissioning of Personal Computers

(b) Access and Privacy Policy

(c) Access and Privacy Procedures

(d) Data Destruction Standard

(e) Data Destruction Form