UNIVERSITY OF MANITOBA

UNIVERSITY OF MANITOBA
POLICY

Policy:	**CUSTODY AND CONTROL OF ELECTRONIC DEVICES AND MEDIA POLICY**
Effective Date:	June 23, 2015
Revised Date:	
Review Date:	June 23, 2025
Approving Body:	Board of Governors
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 Policy

1.1 The purpose of this policy is twofold:

(a) to manage the risk of exposing the University's electronic Data or licensed software programs to individuals or companies unauthorized to view or utilize the Data or programs;

(b) to manage the financial cost and risk associated with disposing of Electronic Devices.

Part II
Policy Content

2.1 The following terms have the following defined meanings for the purposes of this policy:

(a) **Change in Custody and Control:** the following situations constitute a change in custody and control of an Electronic Device or Electronic Media:

(i) transferring responsibility for an Electronic Device or Electronic Media from one University individual and/or department to another individual and/or department;

(ii) returning an Electronic Device to a vendor (e.g. under a return of merchandise authorization) or leasing company;

(iii) allowing an unmonitored external third party to effect repairs to an Electronic Device or Media; and

(iv) recycling or otherwise disposing of an Electronic Device or Media.

(b) **Clear:** means a method of sanitization that applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported), in accordance with applicable guidelines established by the Chief Information Officer of IST.

(c) **Custodian**: means the individual who is forfeiting custody and control of the Electronic Device or Electronic Media and/or the individual who is responsible for the Data on the Electronic Device or Media; this may be on behalf of a department or unit.

(d) **Electronic Devices:** Any electronic equipment that has a storage device or persistent memory. Such devices may include, but are not limited to, desktop computers, laptops, tablets, servers, personal data assistants, cell phones, printers, copiers, routers, switches, firewall hardware.

(e) **Electronic Media:** Any media on which electronic Data can be stored, including, but not limited to: hard disk drives, solid-state drives, magnetic tapes, diskettes, CDs, DVDs, BRDs (Blu-ray Discs™). Solid-state drives include all solid state hard drives, USB external storage devices, and flash based memory cards.

(f) **Data:** Factual information, used as a basis for reasoning, discussion or calculation; representations of information or of concepts, in any form; raw information in its simplest form. Pieces of information from which “understandable information” is derived.

(g) **Grace Period:** the period of time between forfeiture of custody and control of the Electronic Device or Electronic Media by the Custodian and destruction of the data on the Electronic Device or Electronic Media.

(h) **Purge:** a method of sanitization that applies physical or logical techniques that render Target Data recovery infeasible using state of the art

laboratory techniques, in accordance with applicable guidelines established by the Chief Information officer of IST. .

(i) **Technical Support Representative**: an authorized employee of the University who assists with the set-up, maintenance or decommissioning of Electronic Devices who is either internal or external to Information Services and Technology within the University, including but not limited to IST Service Desk, IST Desk Side Support, faculty assigned IT support, distributed IT staff.

2.2 This policy is applicable whenever there is a pending Change in Custody and Control of the Electronic Device or Electronic Media.

2.3 All software and Data files stored on University owned and/or operated Electronic Devices and Electronic Media that are to be recycled, disposed, permanently returned to a vendor or leasing company, or redeployed within or between University faculties or units must be rendered unreadable using University-approved procedures prior to effecting a Change in Custody and Control.

2.4 When Electronic Devices or Electronic Media are to be temporarily removed from the control and custody of the University (e.g. to facilitate repair by an external party), all Data stored on the Electronic Devices or Media must be encrypted or otherwise rendered unreadable by University-approved procedures prior to effecting the Change in Custody and Control.

2.5 Electronic Devices and Electronic Media that were, at any time, used in in the conduct of the affairs of the University may not be sold to an external party, including present and past employees and students; and

2.6 Donation of Electronic Devices and Electronic Media that were, at any time, used in the conduct of the affairs of the University to an external party, including past and present employees and students of the University) is strictly prohibited unless specifically approved by the University's Chief Information Officer. The Chief Information Officer may, at his/her discretion, approve donation of Electronic Devices and Electronic Media to an external party if the party proposing the donation can reasonably demonstrate that the goodwill is likely to outweigh the inherent cost and risk of making the donation (relative to the standard electronic waste recycling process).

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 Policy is required.

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

3.3 All employees are responsible for complying with this Policy.

Part IV
Authority to Approve Procedures

4.1 The Chief Information Officer, IST may approve Procedures, if applicable, which are secondary to and comply with this Policy.

Part V
Review

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

5.2 In the interim, this Policy may be revised or repealed if:

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

(b) the Policy is no longer legislatively or statutorily compliant; and/or

(c) the Policy is now in conflict with another Governing Document.

5.3 If this Policy is revised or repealed all Secondary Documents, if applicable, shall be reviewed as soon as possible in order that they:

(a) comply with the revised Policy; or

(b) are in turn repealed.

Part VI
Effect on Previous Statements

6.1 This Policy 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 VII
Cross References

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

(a) Custody and Control of Electronic Devices and Media Procedure

(b) Requisition to Destroy Records

(c) Requisition to Transfer Records (RTR)

(d) *The Freedom of Information and Protection of Privacy Act*

(e) *The Personal Health Information Act*