EPIGENOME TECHNOLOGIES

Data Destruction and Sanitization Policy

1. Overview

Epigenome Technologies Inc. regularly stores sensitive information on computer hard drives and other forms of electronic media. As new equipment is obtained and older equipment and media reach end of life, sensitive information on surplus equipment and media must be properly destroyed and otherwise made unreadable to protect Confidential Information or Personally Identifiable Information (PII).

2. Purpose

Proper disposal and disposition of surplus computer hardware and other storage media manages risks of security breach and inappropriate information disclosure. Broadly, exposure to the agency takes the form of:

- **Violation of Software License Agreements** - Most software is licensed for use on either a single computer system, to a single person, or to an organization. Typically, licenses are not transferable. Even when licenses are transferable, there are generally specific requirements that must be met in order to affect a transfer. Allowing a third party access to licensed software without proper transfer of the license may be a breach of the license agreement, and may subject the state or the recipient of the software to claims and/or damages.

- **Unauthorized Release of Confidential Information or PII** - Allowing an unauthorized person access to Confidential Information or PII can subject Epigenome Technologies Inc. to claims for damages.

This policy is designed to address proper disposal procedures for Confidential Information and/or PII from Epigenome Technologies Inc. surplus assets prior to their disposal. Proper sanitization and disposal procedures are key to ensuring data privacy and license compliance.

3. Scope

This policy applies to all Epigenome Technologies Inc. staff.

4. Policy

A. GENERAL

The transfer or disposition of data processing equipment, such as computers and related media, shall be controlled and managed according to HIPAA guidelines. Data remains present on any type of storage device (whether fixed or removable) even after a disc is “formatted”, power is removed, and the device is decommissioned. Simply deleting the data and formatting the disk does not prevent individuals from restoring data. Sanitization of the media removes information in such a way that data recovery using common techniques or analysis is greatly reduced or prevented.

B. DATA DISPOSAL PROCEDURES

All computer desktops, laptops, hard drives, and portable media must be processed through IT department for proper disposal. Paper and hard copy records shall be disposed of in a

secure manner as specified by the archiving and destruction policy. The IT manager shall ensure procedures exist and are followed that:

- Address the evaluation and final disposition of sensitive information, hardware, or electronic media regardless of media format or type.
- Specify a process for making sensitive information unusable and inaccessible. These procedures should specify the use of technology (e.g. software, special hardware, etc.) or physical destruction mechanisms to ensure sensitive information is unusable, inaccessible, and unable to be reconstructed.
- Authorize personnel to dispose of sensitive information or equipment. Such procedures may include shredding, incinerating, or pulp of hard copy materials so that sensitive information cannot be reconstructed. Approved disposal methods include:
    - **Physical Print Media** shall be disposed of by one (or a combination) of the following methods:
        - *Shredding* - Media shall be shredded using Epigenome Technologies Inc. issued cross-cut shredders
        - *Shredding Bins* - Disposal shall be performed using locked bins located on-site using a licensed and bonded information disposal contractor
        - *Incineration* – Materials are physically destroyed using licensed and bonded information disposal contractor
    - **Electronic Media** (physical hard disks, flash drives, printer and copier hard-drives, etc.) shall be disposed of by one of the methods:
        - *Overwriting Magnetic Media* - Overwriting uses a program to write binary data sector by sector onto the media that requires sanitization
        - *Degaussing* - Degaussing consists of using strong magnets or electric degaussing equipment to magnetically scramble the data on a hard drive into an unrecoverable state
        - *Physical Destruction* – implies complete destruction of media by means of crushing or disassembling the asset and ensuring no data can be extracted or recreated

IT documentation, hardware, and storage that have been used to process, store, or transmit Confidential Information or PII shall not be released into general surplus until it has been sanitized and all stored information has been cleared using one of the above methods.

5. Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of the Epigenome Technologies Inc. internal application development and release methodology. Examples of control documentation includes:

- On-demand documented procedures related to surplus disposal of hardware and software

- Data destruction and surplus logs of equipment identified for disposal
- Physical evidence of sanitized assets and/or data destruction/cleansing devices

6. Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

7. Distribution

This policy is to be distributed to all Epigenome Technologies Inc. staff handling sensitive hard copy documents or responsible for managing data and hardware assets in the organization.

8. Policy Version History

Version	Date	Description	Approved By
1.0	5/01/2022	Initial Policy	