Mobile Device, Peripheral Device & Removable Media Policy

Purpose & Scope

This Policy applies to all Epigenome Technologies employees, and all devices capable of communicating with the Epigenome Technologies network or attached devices via USB, Bluetooth, TCP/IP, UDP, or any other communications protocol. This includes, but is not limited to: USB memory sticks, portable music players, personal digital assistants, cell phones, microphones, cameras, headsets, keyboards, and mice.

All devices capable of interfacing with the Epigenome Technologies network, including peripheral devices or removable media connected to computers with network access, pose a risk of installing or transmitting malware, corrupting or destroying data, or providing unauthorized access to confidential information. As such, this policy seeks to regulate the devices used to (i) access Epigenome Technologies web services (ii) connect to the Epigenome Technologies network, or (iii) provide media or peripheral capabilities on devices that perform (i) or (ii).

Devices used by employees of Epigenome Technologies for strictly personal use are not subject to this policy.

The Chief Executive Officer is the final authority for this policy.

Policy Statement

Definitions

A **Mobile Device** is any device used to connect to the Epigenome Technologies network, or to access online resources managed by Epigenome Technologies, including email and online data storage. Examples of mobile devices include laptops, smartphones, and tablets.

A **Peripheral Device** is any device used to connect to an Epigenome Technologies computer, or to a Mobile Device. Examples of peripheral devices include Bluetooth headsets, USB speakers, or external keyboards.

A **Removable Storage Device** is any device used to transfer data from Epigenome Technologies or a Mobile Device. Examples of Removable Storage include USB sticks, smart phones, and wireless hard drives.

A device may be covered under multiple sections. For instance, an iPhone can be used to read corporate email (Mobile Device), play music through computer speakers (Peripheral Device), and drop files for backup or transfer (Removable Storage).

Mobile Devices

It is the responsibility of each employee of Epigenome Technologies who uses a mobile device to access Epigenome Technologies resources to ensure that these devices are both physically and electronically secure. This means:

- All mobile devices must be protected by a strong password or by a PIN of 8+ digits
- All uses of mobile devices must comply with the Data Protection & Privacy Policy and the Nondisclosure & Confidentiality Policy
- All employees must employ reasonable physical security measures to protect their mobile device against being lost or stolen
- All mobile devices will routinely install system updates and patches to ensure against known exploits
- The loss or theft of a mobile device must be reported to Epigenome Technologies within 1 business day

Removable Storage

It is the responsibility of each employee of Epigenome Technologies to ensure that data stored on removable storage is (1) Non-confidential and (2) Inaccessible to outside actors; as such:

- No confidential information shall ever be stored on removable storage in any form
- No passwords shall ever be stored on removable storage in any form
- Password-capable devices (such as smartphones) must have this capability turned on, and a strong password or PIN of 8+ characters used
- Password-incapable devices (such as USB sticks) must be encrypted at the disk level, or store only encrypted files
- All employees must employ reasonable physical security measures to protect their removable storage device or its contents against being lost or stolen
- The loss or theft of a Removable Storage Device must be reported to Epigenome Technologies within 1 business day

Peripheral Devices

It is the responsibility of each employee of Epigenome Technologies to ensure that peripheral devices connected to Epigenome Technologies infrastructure, or to any device interacting with Epigenome Technologies infrastructure, do not promulgate malicious software or scripts, including malware, ransomware, and spyware. To this end:

- All peripheral devices shall be obtained from a reputable source, e.g., standard retailer
- Peripheral devices shall only be used to connect to Epigenome Technologies infrastructure, or to Mobile Devices as defined above
- Peripheral devices shall not be shared between employees and non-employees
- All employees must employ reasonable physical security measures to protect their peripheral device against tampering
- The loss or theft of a peripheral device may be reported to Epigenome Technologies