PIEAS USB Security Policy

1.0 Purpose

USB Flash Drives have gained popularity due to their huge data storage capacity, simplicity of use and portability. The problem with portable devices, however, is their vulnerability to theft and eventually data theft. The use of USB Flash Drives might simplify life but unless adequate security measures are taken, the organization is left vulnerable to not only the threat of data loss but of legal action from the affected parties.

USB flash drives are widely used by researchers, instructors and support staff to transport PowerPoint instructions, learning and research material, data related to meetings and lectures, and work in progress between office and home.

2.0 Scope

This policy applies to all staff (officers/staff/students/visitors) employed by or working on behalf of PIEAS. A security policy being adopted by an organization means that all its staff members are obligated to follow the basic steps required to ensure safety of their laptops and USB Flash Drives.

3.0 Policy

3.1 General Security Policy

Some of the best practices for formulating a USB Flash Drive Security Policy include:

- Ensure that your USB flash drive encrypts the data as soon as it is stored in the device with the full disk encryption feature. This will not only restrict the use of the drive to computers that have compatible encryption software but also help avoid unauthorized access to data.
- The data stored on a USB flash drive should be put through regular audit trial.
- Organizations should circulate notices to all the mobile device users to restrict the use of USB flash drives at particular places.
- Make all USB flash drives password protected in order to thwart unauthorized access of the confidential data.
- USB flash drives also come with biometric finger print identification software that helps recognize the legitimate user. The software scans finger prints, authenticates the user and only then allows him/her to access the data.

3.2 Official USB Security Policy

- The IT Coordinator, PIEAS, in collaboration with PIEAS Stores and the administration will manage a record of all official issued to officers and staff within the organization to keep a track of the use of these devices inside and outside the PIEAS network.

- In case of a store issue, PIEAS Stores will ensure that the name of entity against whom name USB is being issued is brought in the knowledge of the PIEAS IT Coordinator. The IT coordinator will update the official record.

- In case of a store return as serviceable or unserviceable, PIEAS Stores will ensure that the returning entity/officer has got the USB delisted from the official record by bringing it in the notice of IT Coordinator through a formal request through email or latter.

Document Title	PIEAS USB Security Policy
Document Category	Policy
Scope of the Policy	This policy applies to all users of computing resources owned or managed by PIEAS. Individuals covered by the policy include (but are not limited to) PIEAS faculty and visiting faculty, staff, students, alumni, guests or proxies, external individuals and organizations accessing network services via PIEAS' computing facilities.
Date of Origin/Version	June 16, 2013/Version 1.0
Last Revision/Version	November 3, 2014/Version 3.0
Author	CISD
Owner	CISD
Approving Authority	Rector PIEAS
Date Authorized	November 03, 2014
Effective From	November 03, 2014
Change Control Board	Rector PIEAS Pro-Rector PIEAS Head CISD IT Coordinator Network Administrator Mail Administrator WebMaster