Restricted Use Data
Clean Desk and Clear Screen Policy

1.0 Overview

The purpose for a Restricted Use Data Clean Desk and Clear Screen policy is to establish a culture of security and trust for employees at WPI. An effective clean desk and clear screen effort involving the participation and support of WPI employees can greatly protect paper and electronic documents that contain Restricted Use Data about our students, employees, donors, alumni, parents, and friends. All employees that handle Restricted Use Data should familiarize themselves with the guidelines of this policy.

2.0 Scope and application

This policy applies to all university workforce members that handle Restricted Use Data. This policy covers any papers, screen displays, removable storage media and any computing devices that contain or display University Restricted Use Data regardless of location.

3.0 Policy

At known extended periods away from your desk, such as lunch breaks or meetings, working papers containing Restricted Use Data should be placed in locked drawers or a locked office and screen displays should be placed in a locked screen state.

At the end of the working day, an employee should tidy his or her desk and put away all office papers that contain Restricted Use Data, secure all screens **and** lock his or her office. WPI provides locking desks and filing cabinets for this purpose.

Actions

1. Allocate time in your calendar to clear away your Restricted Use Data paperwork.
2. Always clear your workspace of Restricted Use Data paperwork before leaving for long periods of time.
3. Whenever unattended or not in use, all computing devices that can be used to display Restricted Use Data must be logged off or protected with a screen or keyboard locking

mechanism controlled by a password or similar user authentication mechanism, (devices include laptops, tablets, smartphones, and desktops).

4. Paper containing Restricted Use Data must be removed from printers and faxes immediately. Faxes and printers used to print Restricted Use Data should not be in public areas. Any time a document containing Restricted Use Data is being printed the user must make sure they know the proper printer is chosen and also go directly to the printer to retrieve the document.
5. If in doubt - check with your supervisor. If you are unsure of whether a duplicate piece of Restricted Use Data documentation should be kept or even produced - discuss it with your supervisor before shredding.
6. Restricted Use Data on paper or electronic storage media that is to be shredded must not be left in unattended boxes or bins to be handled at a later time and must be secured until the time that they can be shredded.
7. Destroy Restricted Use Data documents when they are no longer needed through cross-cut shredders or locked shredder boxes.
8. Lock your office, desk and filing cabinets that contain Restricted Use Data at the end of the day. Don't keep the keys in the lock or drawer.
9. Portable computing devices such as laptops smartphones and tablets that can be used to display Restricted Use Data should be secured in a locked office or cabinet at the end of the day.

Tips to Keeping a Clean Desk

- Lock your office door when you're gone for extended periods; if you don't have an office, lock your cabinets. Do not leave keys in their locks.
- Never leave your access cards or keys out anywhere; always keep them with you; notify University Police immediately if access cards or keys are missing.
- Lock your computer when you leave your desk for an extended period of time, including overnight.
- Do not leave portable media with Restricted Use Data, such as optical disks, USB flash drives or portable hard drives, out or attached to your computer.
- Enable and use a password-protected screen saver.
- Never write your passwords on a sticky note nor try to hide them anywhere in your office.
- Remove printouts containing Restricted Use Data from printers before leaving your office.
- Shred Restricted Use Data printouts when you are done with them using a cross-cut shredder or locked shredder bin.
- Clear cache files on your computer regularly.

- Do not use bookshelves to store binders with Restricted Use Data. Label those binders accurately and lock them up.

4.0 WPI Information Security Roles

CHIEF INFORMATION SECURITY OFFICER
Worcester Polytechnic Institute
100 Institute Road
Worcester, MA 01609
Phone: (508) 831-5115
Fax: (508) 831-5483

5.0 Enforcement

Any person that violates any of the measures found in this policy will be subject to the same disciplinary actions outlined in WPI's Confidentiality Agreement for employees, or the Acceptable Usage Policy and Code of Conduct for students.

6.0 Approval and Revisions

Policy Category: Institutional Risk & Compliance

Policy Approved By: Approved by WPI's Information Security, Risk and Compliance Committee on 11/06/2018.

Policy Reviewed Annually By: Chief Information Security Officer

Related University Policies:

Data Classification and Usage Policy
Mobile Device Policy

Last Modified: 10/31/2018