what is PIMI?

The Private Information Management Initiative (PIMI) is a program to help identify and remove private information (PI) from RIT computers and attached drives. To do this, the RIT Information Security Office uses Identity Finder software to scan all faculty and staff computers connected to the RIT network. The software scans items looking for specific patterns of numbers that match patterns for common private information.

If Identity Finder locates suspected PI on your computer, it will create a report for you to view and take action on. This report contains tools for you to scrub or shred files containing PI. This report also goes to the RIT Information Security Office who will follow up with you as needed regarding the PI found.

what is my responsibility?

- Allow Identity Finder Scans to run
- View the report and take action on the matches

You cannot just hide PI, you must remove it. If there is a business reason for you to keep PI, contact your business representative.

what information is considered private?

RIT scans for data such as Social Security numbers (SSN), driver's license numbers, account numbers, and credit or debit card numbers.

INFORMATION SECURITY

what if I have other questions?

Read our FAQs at: https://www.rit.edu/security/content/private-information-management-initiative-pimi-faq

Or contact your PIMI Representative.

get informed

Visit the RIT Information Security website to view additional resources about the initiative.

RIT INFORMATION SECURITY

http://rit.edu/security

infosec@rit.edu

(585) 475-4123

private information management initiative (PIMI)

Your Responsibilities

INFORMATION SECURITY

Revised 9/17/2013

how do I remove private information?

On the report from Identity Finder, select one of two options to remove the PI:

- Scrub = securely remove the PI data from a file you want to keep
- Shred = securely erase the entire file

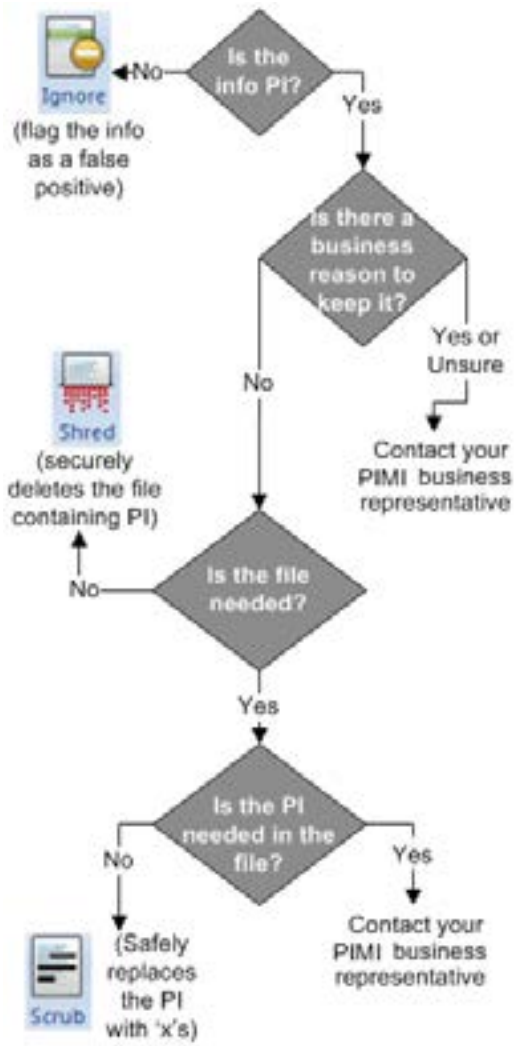
For detailed instructions visit:

- **MACS:** https://www.rit.edu/security/sites/rit.edu.security/files/MAC%20End%20User%20Guide%20v2%205.pdf
- **PCS:** https://www.rit.edu/security/sites/rit.edu.security/files/IDFUserguide.pdf

what if the matches found are not actually private information?

Sometimes Identity Finder flags data that is structured or has a length similar to true PI. If Identity Finder marks data as private that is not actually private, you can use the report to mark these "false positives" as **Ignore**. The RIT Information Security Office may review these ignored items to ensure they are not PI.

how do I know what to do?



You can also reference our quick handling guide: https://www.rit.edu/security/content/private-information-handling-quick-reference-table.

why is PIMI important?

This initiative will help reduce the amount of PI at RIT, creating a safeguard against identity theft. PIMI also helps RIT comply with relevant state and federal laws.

RIT is authorized to scan any RIT computer using the RIT network in order to protect the RIT community and help users comply with the Information Access and Protection Standard.

who can I contact?

Each organization has PIMI Representatives:

- Technical Representative – assists with technical issues and installation of Identity Finder
- Business Representative – coordinates with Information Security Office to ensure resolution, provides guidance on remediation

Specific details on who is a representative for your organization can be found: http://www.rit.edu/security/content/PIMIReps