## Using Identity Finder

To find and secure personal information on your computer, the Information Security Group recommends that you install and periodically run Identity Finder (IDF), which helps prevent identity theft and aids in keeping Brown compliant with federal and state laws by detecting and securing sensitive data on your computer. IDF is able to detect patterns – such as those for Social Security, credit card and bank account numbers, references to passwords and other customizable data that you would specify.

All active employees – faculty and staff – can download and install the full enterprise version of IDF from the Software download pages onto their Brown computers (runs on both Windows and Macs). In addition, software is available from the Identity Finder website for use by students and home users, including a free application, Password Sweeper.

□ Install Identity Finder. Faculty and staff can download IDF from the Software Catalog. A link is also available at brown.edu/go/identityfinder. Versions for students and home use – Password Sweeper (free), Identity Sweeper (\$29.95) and Identity Sweeper Pro (\$39.95) – can be found at identitysweeper.com/products.

Catalog	Search	Apply			
Windows	identity finder				
Macintosh	10 <b>1</b> 0				
Linux	TITLE	DESCRIPTION	OPERATING	LICENSED FOR	
Apple iOS (mobile)	11111				
Deprecated				Staff	
	Identity Finder	Detects and secures sensitive data on your personal	Windows	Staff	

**Follow the Setup Wizard to activate the software** (installation instructions can be found on the download page) then create a password to secure your reports.

i 🖟 Identity Finder Setup	Identity Finder Profile Password X
Welcome to the Identity Finder Setup Wizard           This wizard will guide you through the installation of Identity Finder 6.2.           identityfinder	Vew Identity Finder Profile         Your Profile allows you to save your settings and automatically use your Profile Password when securing results or saving reports. You will be asked for this password when Identity Finder statts and when opening secure results and reports.         Enter Password:       Image: Confirm Password         Confirm Password:       Image: Confirm Password         identity finder       Image: Confirm Password
< Back Next > Cancel	Next> Cancel Help

Define your search: what drive(s), types of files, kinds of PII. To meet regulatory compliance, ISG recommends searches of your hard drive that target social security and credit card numbers. This data is at highest risk and searches for it produce the fewest false positives.

	Nain Identities Locations Configuration Tools
Configure your search to locate credit card	Files       Files <td< td=""></td<>
numbers and SSNs.	Solution </td
	Social Credit Card Entry Card Entry Account License Birth Number Address Address
	AnyFind

Protect any discovered PII by destroying or securing it (Shred, Scrub, Secure and Quarantine).

File	Main	Identi	ties L	ocations	Confi	guratior	n To	ols		
		<b>P</b>					¥		3	
Start *	Stop	Filter Results	Collapse All Rows		Shred	Scrub	Secure *	Quarantine	Recycle	Ignore *
Searc	h 🔤		Display				Act	ions		- G

Schedule regular runs. How often depends on what kinds of PII you routinely deal with. If you handle SSNs and bank account information in your daily work, ISG recommends once a week, and if otherwise, quarterly at a minimum. Note that you may wish to broaden your search to other sensitive information, such as passwords, after initial scans for high risk PII.

		Task Schedule 83
Settings	2	A search will automatically run according to the schedule you set below. You will be required to enter the username and password that you use to log on to Windows.
Databases  Custom Folders	Change the options for scheduling a search	Schedule Task: Start Time:
Remote Machines	Schedule a search to run automatically	Schedule Task Weekly
Ignore	Schedule a search: Configure	Every 1 🖕 week(s) on: Mon 🖉 Sat
Scheduling	Configuration Settings:	Tue Sun
Logging a	Use Profile settings	🗌 Wed
Resources	Use other settings: ①     Copy Current       ① Use configuration file:	
	OK Cancel Apply Help	Set Password OK Cancel

For questions about using the software, visit **brown.edu/go/identityfinder**, which includes links to the online manuals for both Windows and Macs. The page also includes recommendations on when to use the various protection options with examples of each. For questions about policy and/or procedures, contact <u>ISG@brown.edu</u>.

prepared by the **Information Security Group** ISG@brown.edu | brown.edu/go/isg | twitter.com/ISGatBrown last revised 12/12/2014