



P.O. Box 26833
San Diego, CA 92196
858.693.7935
www.idtheftcenter.org

The Identity Theft Resource Center

Data Collection and Record Retention POLICY

The Identity Theft Resource Center takes seriously its obligations to preserve information relating to litigation, audits, and investigations. The Sarbanes-Oxley Act makes it a crime to alter, cover up, falsify, or destroy any document to prevent its use in an official proceeding. Failure on the part of employees to follow this policy can result in possible civil and criminal sanctions against ITRC and its employees and possible disciplinary action against responsible individuals (up to and including termination of employment). Each employee has an obligation to contact the chief executive or chief financial officer of a potential or actual litigation, external audit, investigation, or similar proceeding involving ITRC. The information listed in the retention schedule below is intended as a guideline and may not contain all the records ITRC may be required to keep in the future. Questions regarding the retention of documents not listed in this chart should be directed to the chief executive. From time to time, the chief executive may issue a notice, known as a “legal hold,” suspending the destruction of records due to pending, threatened, or otherwise reasonably foreseeable litigation, audits, government investigations, or similar proceedings. No records specified in any legal hold may be destroyed, even if the scheduled destruction date has passed, until the legal hold is withdrawn in writing by the chief executive.

Data Collection

The data collection policy of the ITRC shall be maintained on two levels:

Level 1:

This is data which is collected for the purposes of assisting general victims of identity theft. This shall consist of name, state of residence, phone number, and/or e-mail address. A street address may be collected for the purposes of mailing information to the individual to assist them with their case.

This is also data that is collected for the purposes of studies or research. Upon completion of gathering of data, the personal identifying information shall be separated and maintained in a secure manner. Upon completion of this study or research all such data shall be destroyed. During the research phase, some individuals request to do media. At this time they volunteer their information, which is entered, as appropriate, into Salesforce. We do not release the victim’s information to the media. It is the policy of the ITRC to provide the media contact information to the victim so that the victim may initiate the contact with the media.

Level 2:

This is data that is collected or supplied by the victims for the purposes of criminal or advanced identity theft case assistance. This data shall only be collected upon the approval of a member of the ITRC management team. Data in this category could consist of Social

Security numbers, date of birth, drivers license number, financial account numbers, health insurance numbers, employee identification numbers, or any data determined to be of a more uniquely personal identifying nature.

Level 2 data shall not be stored electronically but converted to hard copy paper files to be stored in an appropriately labeled file in the office of the Executive Director. The Level 2 data file storage in the Executive Director's office shall be referred to as the "ITRC Case Vault", and shall remain locked except when in use. Access to the ITRC Case Vault and the Executive Directors office shall be restricted to the management team and the appropriate victim advisor.

Storage:

ITRC will maintain Level 1 data in electronic form using Salesforce, a database program specially designed for enterprise business services. The Salesforce database used by ITRC is accessible only by ITRC staff, with permissions regulated strictly by individual login. Safeguards for the protection of electronic files include both hardware and software firewalls, use of SSL technology for all connections, verified IP for all connections, and discrete user tokens on each user machine, as well as user name and password protection. Level 1 information can include name, state of residence, phone number, and/or e-mail address, and in some cases city and street address.

Other ITRC files, such as email, company business files, etc., are to be stored in electronic form on the ITRC file server, in an access controlled room, within the ITRC facility. They are protected by appropriate firewalls and intrusion detection. External access to the server is limited to secure VPN only.

Level 2 data, which can contain specific PII such as Social Security number, shall not be stored in electronic form, but committed to paper for controlled storage. Extremely sensitive personal identifying information, e.g., Social Security numbers, will not be collected unless necessary in order to effectively assist a victim in restoration of his or her identity (Level 2 data). When it is necessary to collect such sensitive information, it should not be stored in electronic format at all, but kept as paper copy only within the ITRC case vault. This vault is locked, and within a room with separate limited access.

Disposal:

Procedures for the final disposition of data: Because ITRC undertakes an advisory role with victims of identity theft, and because the nature of this crime may require years for mitigation, victims have the expectation that ITRC will retain for safekeeping and future access any case information that may be of use to the victim's case in the future. ITRC has the ability to store client files for safekeeping indefinitely in a secure, locked storage unit housed in the same building as the ITRC offices. Data will be retained for a minimum period of three years and/or destroyed at the request of the client.

Responsible Parties for disposition of data:

Jay Foley, Executive Director
Rex Davis, Director of Operations
Sheila Gordon, Director of Victim Services

Retention:

Information will be retained by the ITRC according to the following schedule:

File Category	ITEM	Retention Period
Corporate Records	Bylaws and Articles of Incorporation	Permanent
	Corporate Resolutions	Permanent
	Board and Committee Meeting Agendas and Minutes	Permanent
Finance and Administration	Conflict of Interest Disclosures	4 Years
	Financial Statements Audited	Permanent
	Auditor Management Letters	Permanent
	Payroll Records	Permanent
	Journal Entry	Permanent
	Check Register and Checks	7 Years
	Bank Deposits and Statements	7 Years
	Charitable Org Registrations	7 Years
	Chart of Accounts	7 Years
	Expense Reports	7 Years
	General Ledgers and Journals	7 Years
	Accounts Payable Ledger	7 Years
	Investment Reports	7 Years
	Equipment Files	5 Years
	Contracts and Agreements	7 Years from end of term
Insurance Records	General Correspondence	3 Years
	Policies - Occurrence Types	Permanent
	Policies - Claims Made	Permanent
	Accident Reports	7 Years
	Fire Inspection Records	7 Years
	Safety OSHA Reports	7 Years
	Claims after settlement	7 Years
Group Disability Records	7 Years from end of benefit	
Real Estate	Deeds	Permanent
	Leases Expired	7 Years from end of term
	Mortgages and Security	7 Years from end of term
	Purchase Agreements	7 Years after disposal req's.
Tax	IRS Exemption Determinations	Permanent
	IRS 990	Permanent
	Withholding Tax Statements	7 Years
	Accountant or Legal Correspondence	7 Years after filing.
	Time Cards	3 Years
Communications	Communication Documents	Onsite and Offsite Copies
	Press Releases	Permanent
	Annual Reports	Permanent
	Other Publications	7 Years
	Photos	7 Years
	Press Clippings	7 Years
Donor Services	Fund Agreements, Papers, Copies	Permanent
	Correspondence, Gifts, Grant Req's.	Permanent
Consulting Services	Consulting Contracts	7 Years from end of term
Human Resources	Employee personal files	Permanent
	Retirement Plan Benefits	Permanent
	Employee Medical Records	Permanent
	Worker Comp Claims	7 years after settlement
	Employee Orientation and Training	7 years from use
	Employment Offer Letter	7 years from use
	Employment Applications	3 Years
	IRS Form I-9	3 Years / 1 Year after service
	Resumes	1 Year
Technology	Software Licenses and Support	7 Years after end of obligations
	CEO Correspondence	7 Years
General Administration	CEO Calendars	7 Years

Signature _____ Date _____

Name (please print) _____