Version 7- September 2012

Contact Name:
Company Name:
Contact Phone Number:
Address:
Date sent to company:

CODE OF PRACTICE

NZSA NEW ZEALAND SECURITY ASSOCIATION

Secure Storage and Destruction of Sensitive Material

FOREWORD

This Code of Practice defines the policies and procedures to be followed by members of the New Zealand Security Association involved in the Secure Storage and Destruction of Sensitive Material.

The objective in preparing this document is to ensure that high professional standards are maintained, legal responsibilities complied with and, consequently, enhancement of the industry's image and reputation.

The requirements of this Code are mandatory and compliance is a condition of membership of the New Zealand Security Association.

© 2004 NEW ZEALAND SECURITY ASSOCIATION (INC.)

First Print:	December 1989
Revised and Reprinted:	April 1991 & April 1998
Reprinted:	November 2002
Revised:	May 2006
Revised:	November 2006
Revised:	September 2012

© COPYRIGHT
The copyright of this document is the property of the New Zealand Security Association. No part of it may be reproduced by photocopying or by and other means without the prior written permission of the executive Director of the New Zealand Security Association, unless the circumstances are covered by the exemption section (19 and 21) of the Copyright Act 1962.

INDEX

SECTION 1: COMPANY INFORMATION

DESCRIPTION	EVIDENCE
1.1 Company Details **1.1.1 Name**	
1.1.1 (a)Trading name(s)	
1.1.1.(b) Company Registration details (date and registration number) ***Auditor to sight Company Registration Certificate***	
1.2 Directors (list) ***Auditor to check against Companies Office records.***	

DESCRIPTION	EVIDENCE
1.3 Staff Numbers **Total:** **1.3 (a) Numbers required to hold CoAs:**	
1.4 Registration under the Private Security Personnel and Private Investigators Act 2010 (& Amdts and Replacements) Where there is a requirement to be licensed or hold a Certificate of Approval (COA) all Directors, Staff and/or Contractors are registered under the Private Security Personnel and Private Investigators Act 2010 and amendments. ***Auditor is to:*** • ***Sight SG Licence issued by the Registrar*** • ***Check the COA for a range of not less than five staff.*** • ***Check at least three rosters for duty to ensure all staff working are licensed correctly.***	

DESCRIPTION	EVIDENCE
1.5 Contractors to the Member Company The primary contractor (the member) is responsible to ensure that all contract staff employed under any contractual arrangement are licensed or hold Certificates of Approval as required under the Private Security Personnel and Private Investigators Act 2010 and amendments. All contractors are to be required to show evidence to their principal that they have sufficient processes in place to ensure this requirement is always met. ***Auditor is to:*** • ***Sight the SG Licence issued by the Registrar to the Contractor*** • ***Check the Contractor's staff for current COAs - not less than 10% of member's staff.*** • ***Check at least three rosters for duty to ensure all staff working are licensed correctly.*** • ***Check members' written evidence that all contracted staff are required to hold a current SG licence and/or COA as required under the Private Security Personnel and Private Investigators Act 2010 and amendments***	
1.6 Company Structure The member organisation is to have a definitive governance and management structure that demonstrates control and accountability at each level of its operations ***Auditor is to obtain a clear picture of the corporate structure, levels and controls in place***	

DESCRIPTION	EVIDENCE
1.7 Financial The member organisation is required to have sufficient capital to meet operational and anticipated needs. ***Auditor is to obtain a signed statement from the owners/directors confirming this.***	
1.8 Insurance Members providing Secure Destruction services shall have appropriate cover in the following areas: • Professional Indemnity Insurance • Public Liability Insurance Professional indemnity insurance and public liability insurance cover required of all NZSA members shall have due regard to the nature of the risk and the relevant standard but shall not be less than $1,000,000. ***The Auditor is to:*** • ***Sight a placement slip, insurers policy document or invoice from an insurer showing the required insurance cover is in place and current.***	
1.9 Locations List all locations you operate from within New Zealand ***Where the company operates from multiple locations the auditor will visit the Head Office and a sampling of branches. This sample must be sufficient to confirm consistency in performance.***	

DESCRIPTION	EVIDENCE
1.9.1 Head Office The company will have an administrative office where all records and business documents are stored in a secure manner. ***Auditor to visit this office to confirm***	
1.10 Customer Service Levels This Code of Practice is issued in order to ensure that persons and organisations operating in the security industry provide a standard of service and quality of employee that meets the standard as defined in this Code of Practice as being the minimum level. Sufficient latitude is built into the Code to enable Security Companies to exercise initiative and individual expertise in the provision of service to a higher degree than that laid down in the Code. Feedback from end users of member's services should confirm the appropriate levels of customer service. ***Auditor is to:*** • ***Cite any examples of letters from clients praising individual staff or the company for provision of excellent standards of customer service.*** • ***Look for examples of training, posters, briefing notes, bonuses or recognition for staff to deliver excellent customer service.***	

DESCRIPTION	EVIDENCE
1.11 Sale of Services When contacting potential clients callers must clearly identify the organisation they represent. No such calls shall use fear as a sales technique nor give misleading information. Where a contractor or shared service is to be used this must be made clear to the potential client. ***Auditor is to speak with sales staff to confirm.***	

SECTION 2: RECRUITING, VETTING AND APPOINTMENT OF STAFF

DESCRIPTION	EVIDENCE
2.1 Employment Applications In every case applicants for employment will be required to complete an application form on which they will declare details of their previous employment or other activities for up to seven years or back to school leaving as applicable ***Auditor is to:*** • ***Where applicable – check that the following pre-employment checks are being completed.*** • ***Sight the procedures to ensure this information is correctly handled under the Privacy Act.***	
Pre - Employment Checks	
2.2 References Character references are to be called for from not less than two persons nominated by the potential employee and from any immediately previous employers. An offer of employment may be rescinded on the basis of a negative reference check or one which reveals material undisclosed facts by the employee in his or her employment application. ***Auditor is to:*** • ***Sight evidence that references are checked and verified for at least two employees.*** • ***Sight written references for at least two employees (note that these are not always provided by all employers).***	

DESCRIPTION	EVIDENCE
2.3 Character Check The Member shall employ only persons of good character and integrity. If a candidate applies for a position prior to having been issued with a Certificate of Approval then the potential employer shall, as a minimum, conduct a criminal history check. ***Auditor to review standard recruitment process.***	
2.4 Creditworthiness check A creditworthiness check is to be enabled within employment agreements. Where such checks are completed, a copy of the result is to be placed on the personnel file of the employee. After the initial check it is recommended that creditworthiness checks be conducted on a regular basis. ***Auditor is to:*** • ***Sight that the employee contract documentation allows for pre-employment and annual credit checks.*** • ***Where applicable – check the current credit checks are being completed.*** • ***Sight the procedures to ensure this information is correctly handled under the Privacy Act.***	
2.5 Non-New Zealand Citizen If a non-New Zealand citizen makes an application to become a staff member the employer shall ensure by reference to the individual's passport and/or Labour Department work permit that the applicant may legally be employed in New Zealand. ***Auditor is to:*** • ***View process used to ensure that staff may be legally employed in New Zealand*** • ***Sight evidence that visa checks have been conducted for recently engaged staff.***	

DESCRIPTION	EVIDENCE
2.6 Driving Licences All staff required to drive a motor vehicle during the course of their duties shall be the holders of an appropriate and current New Zealand driving licence. Such a licence must be a full and unrestricted New Zealand Driving licence. ***Auditor is to:*** • ***Sight not less than three driver licence checks made on current employees who are required to drive Company vehicles as part of their duties.***	
2.7 Recruitment Interviews A personal interview will be conducted as part of the recruitment process to determine the candidate's suitability for the role. ***Auditor to review standard recruitment process.***	
2.8 Communication skills All applicants for employment must demonstrate an acceptable level of both spoken and written English. ***Auditor is to:*** • ***Check that the company has procedures in place to determine this as part of the employment process*** • ***Speak to at least two staff in the above category to verify that their spoken English is comprehensible and they are able to understand instructions and requests for information from the general public*** • ***Sight at three examples of written reports or instructions or messages written by any non-New Zealand staff or New Zealand staff for whom English is a second language employed by the member to verify that their written work is legible and understandable to the general public.***	

DESCRIPTION	EVIDENCE
2.9 Physical Fitness All applicants are to make a written declaration that their general health and physical fitness will not provide an impediment to them being able to perform the duties expected of this role. ***Auditor is to check that the company has procedures in place to determine this as part of the employment process.***	
Contracts and Agreements	
2.10 Employment Agreements A written employment agreement between the Member and the applicant employee must be entered into prior to commencement of employment. At all times the Company must ensure compliance with the relevant statutory requirements in relation to employment legislation. The agreement must contain the following: a) Job title b) Roles and Responsibilities c) Effective start date d) Probationary period (if any) e) Pay and allowances f) Hours and days of work g) Holiday entitlement and eligibility h) Sick pay conditions i) The location of the employer's administrative office j) Disciplinary and appeal procedures	

k) Terms of notice and termination. ***Auditor is to:*** • ***Sight at least three employment agreements to ensure they are similar in their provisions of employment*** • ***Sight at least three employment agreements to ensure they are correctly signed and witnessed.*** ***Sight evidence that the employee has been given a copy of their employment agreement.***	
2.11 Non-Disclosure or Confidentiality Agreements Prior to employment all applicants to sign a non-disclosure agreement, maintaining confidentiality of both the company's clients and the company's confidential information. ***Note:*** *Such agreements may form part of the employment agreement.* ***Auditor is to:*** • ***Sight evidence no less than three current staff have signed non-disclosure / confidentiality agreements*** • ***Confirm all applicants signed these forms before acceptance as an employee.*** • ***Check that such agreements cover both client and company information.***	
2.12 Part Time and Casual Staff Where staff are employed on part time and casual contracts the pre-employment checks shall be of no lesser standard than those for full-time employees. ***Auditor is to:*** • ***Sight the guidelines for interviews and staff selection to confirm.*** •	

DESCRIPTION	EVIDENCE
Personnel Files	
2.13 Personnel Files A personnel file shall be established and maintained for all staff employed and is to contain all information relative to each staff member's employment. ***Auditor is to:*** • ***Sight the personnel files to ensure they are secured and access is allowed only to authorised persons in the Company*** • ***Verify that once employees have left, the files are securely destroyed in line with the provisions of the Privacy Act*** • ***Verify that unsuccessful applicant's files are securely destroyed as soon as they are no longer required in accordance with the Privacy Act.***	

SECTION 3: TRAINING

DESCRIPTION	EVIDENCE
3.1 All staff employed by the company shall receive adequate and regular training appropriate to the duties to which they are assigned.	
3.2 Each new employee shall receive basic training in **the** Operational, legal and security aspects relevant to the task taking into account the following: a. PSPPI Act 2010 b. Privacy Act 1993 c. Emergency procedures d. First Aid e. Duties relative to the post to which the staff member is assigned including on-the-job training f. Local and national traffic regulations.	
3.3 Continuation training and the refresher courses should be carried out at least annually on those subjects listed in paragraph 3.2 above. This training should include changes to legislation, safety and security directly related to their area of employment.	
3.4 Records of training are to be maintained on company and personal files noting the subjects dealt with and the date of training. These records shall be maintained during the term of the individual's employment	

SECTION 4: PRACTICES TO BE USED IN THE HANDLING AND TRANSPORTATION OF SENSITIVE MATERIAL

Requirement	Evidence
Handling	
4.1 The most important aspect is that the client's sensitive material will be securely handled while in transit from the client's premises to the secure destruction facility. Until that time the responsibility for the security of the consignment rests with the client. Clients to have the material security packaged for transportation.	
4.2 All sensitive material from the time of collection from the client's premises until destruction at the security destruction facility shall remain in the same sealed security container.	
4.3 It is recommended that sensitive waste be transported in cloth bags, metal or plastic bins or other robust containers, which must be secured with security seals and / or padlocks.	
4.4 The client's sensitive material shall remain secure and sealed within the container it is received in until immediately prior to the destruction process.	
4.5 The sensitive material is to be stored in such a way that it cannot be accessed and information obtained by unauthorised person.	
4.6 Receipts are to be issued to the client for all sensitive material picked up from the client's premises. Receipts are to be on a numbered form and are to quote the security seal number (where applicable) and the name of the security transport officer, date and time of pick up.	

DESCRIPTION	EVIDENCE
4.7 Storage of sensitive material prior to destruction shall not exceed five working days without the express permission of the client. This permission should be in writing.	
4.8 A record is to be maintained at the security destruction facility of all containers received, security seal number (if applicable) and any special comments about the container, bag or bin.	
4.9 A gate log is to be maintained at the secure destruction facility in which a detailed record is made of all access to the secure area including: a. Name of individual and represented company (if any). b. Purpose of visit c. Times of arrival and departure	
4.10 Certificate of Destruction (CD's) having a unique reference number, shall be issued to clients, if requested, for all material following destruction. A CD is to clearly identify the company's facility where the destruction took place. Each CD is to show the actual date of destruction, the method used and the name of the supervisor or destruction operator.	
4.11 CDs must clearly identify the client and material destroyed, quoting seal number in all cases, and is to be signed by an authorised company representative, where destruction is witnessed by a client, and then the client should countersign the CD as a witness.	

DESCRIPTION	EVIDENCE
4.12 A duplicate copy of each CD shall be retained by the company for a period of not less than 12 months after the date of destruction of the material.	
4.13 Invoicing of destruction services to the client is to comply with sound accounting practices and is to clearly identify the material involved.	
Transportation	
4.14 Vehicles used for collecting sensitive material ***must*** be fully enclosed Doors windows and tailgates are to be secured in such a way that loose material cannot fall out	
4.15 The vehicle is to be secured so that illegal entry cannot be effected without the use of force; It is recommended that a 5 Star vehicle alarm system is fitted to protect the vehicles and its contents when it is unattended.	
4.16 When a vehicle is unattended, all doors, windows, and tailgates are to be locked.	
4.17 The security transport operator shall at all times comply with local and national traffic regulations.	
4.18 All vehicles used by security destruction companies in the course of their duties shall bear the company's name, logo or other identifiable marking visible from both sides of the vehicle. The marking shall be of a permanent nature and applied in such a manner that it cannot easily be removed other than by mechanical or chemical means. When vehicle is sold or disposed of all signage is to be removed.	

DESCRIPTION	EVIDENCE
4.19 Where a temporary sub contractor is used, or where specified by a client. The requirement to mark the vehicles as specified in paragraph 7.8 may be waived, in which case the temporary sub contractor must carry an authorisation signed by both the company and the client.	
4.20 Vehicle running sheets or Consignment notes to account for pick-ups are to be maintained. They must show the drivers name, time and date of pick up and client's name and signature plus a seal number (if applicable).	
Personnel	
4.21 All company staff while engaged in the transportation and collection of sensitive material shall wear a readily identifiable uniform bearing the company insignia, which will identify the officer with the company This is not to be worn off duty.	
4.22 All company and sub contractor's staff are to be in possession of an identity card, which, together with their C of A, which identifies them as an authorised security officer.	
4.23 When a company uniform is unfit for further wear, all badges and insignia are to be removed before the disposal. Identity cards that are no longer required for staff members are to be destroyed in a secure manner.	
4.24 The company must recover from staff leaving its employ, all uniforms, insignias, keys, access cards and identity cards and any other items indicating employment with the company.	
4.25 Sub contractors involved in the carriage of sensitive material should not have access to unsecured material.	

SECTION 5: OPERATION OF A SECURE STORAGE AND/OR DESTRUCTION FACILITY

DESCRIPTION	EVIDENCE
5.1 Destruction of sensitive material will be completed on the company's premises in New Zealand in a professional and secure manner that preserves the integrity of the client and the information.	
5.2 The building or vehicle used for the secure destruction facility must be sound with a high standard of Security, maintenance and cleanliness.	
5.3 Secure destruction facilities should be equipped with a combustion (smoke) detection system.	
5.4 Smoke detection systems should be remotely monitored by a monitoring system, which complies with the NZSA Code of Practice for Alarm Monitoring.	
5.5 A fire safety inspection of the facility should be carried out at least annually by a fire safety officer, and certificate issued and displayed.	
5.6 Portable fire extinguishers and / or fire hose reels are to be provided in the building. The company's staff are to be trained in the use of fire fighting equipment provided.	
5.7 The company is to take all reasonable steps to protect the client's records from loss or unauthorised access.	I

DESCRIPTION	EVIDENCE
5.8 The premises must be physically capable of restricting access to protected and restricted areas.	
5.9 The facility is to be protected after hours by an intruder detection system, which is monitored by an alarm monitoring company.	
5.10 The intruder detection system is to comply with the provision of NZS 4301 1993 and the relevant NZSA Code of Practice for the Installation of Intruder Alarm Systems.	
5.11 Alarm conditions reported to the monitoring centre after hours are to have a response by a security guard company licensed under the PI & SG Act 1974.	
5.12 The destruction and storage areas of the building are deemed to be secure areas. During working hours access to the secure areas is to be controlled to prevent unauthorised persons gaining unsupervised access.	
5.13 Visitors (including clients) to the building are to be escorted at all times. Each visitor to the premises is to be positively identified and the date, time and purpose of the visit recorded in a permanent register. The register, when full, shall be retained for a period of not less than 12 months from the date of the last entry.	
5.14 The public and visitors should not be able to view the security precautions of the secure area from either outside the building or from any internal offices or other internal rooms.	
5.15 The company will permit and co-operate with any additional security precautions which a client may wish to implement in addition to those which are specified above. Such additional precautions shall be at client's expense and shall be for the client's exclusive benefit.	

DESCRIPTION	EVIDENCE
5.16 The public and visitors should not be able to read information or identify clients from any material awaiting destruction	
5.17 The company shall have set procedures in place relating to the handling of the breaches of security. Such procedures should be available to clients on request.	
5.18 If the company becomes aware that there has been a breach of security, of disclosure, or potential disclosure, of any sensitive information held on the premises then the client(s) must be informed immediately of the details.	
5.19 The Police are to be informed immediately there is any evidence of a burglary in the secure destruction facility.	

SECTION 6: MOBILE SECURITY DESTRUCTION VEHICLES

DESCRIPTION	EVIDENCE
6.1 Where a company is offering a service involving a vehicle fitted with a security destruction machine that carries out destruction of sensitive material at the client's premises, then the provisions and standards of this Code shall apply with the interior of the vehicle being assumed to be the secure destruction facility without the requirement for alarm monitoring and smoke alarms. It is recommended that a 5 Star vehicle alarm system is fitted to protect the vehicles and its contents when it is unattended.	
6.2 The company shall ensure that the process of transferring the sensitive material to the vehicle is carried out in a secure manner and that containers, bag and bins and also the bulk material are not left unattended at any time during the process.	
6.3 The company shall ensure that the vehicle being used can be parked within 20 metres of the street entrance of the client's premises.	
6.4 The destruction provided shall take place in such a manner that no waste product escapes from the vehicle. Should such an event occur, then the product should be cleaned up before the vehicle leaves the site.	
6.5 The company shall ensure that the operation of the vehicle does not cause excessive noise levels, or the emissions of dust particles, which are likely to cause annoyance to the client and the occupants or surrounding buildings.	
6.6 The Company shall at all times comply with local and national traffic regulations relating to the operation and parking of the vehicle.	

DESCRIPTION	EVIDENCE
6.7 The company shall ensure that climatic conditions do not compromise the security of the process.	
6.8 In the event of a vehicle breakdown or mechanical failure the company must have available alternative arrangements, which comply with this Code.	

SECTION 7: STANDARDS AND METHODS OF DESTRUCTION

DESCRIPTION	EVIDENCE
7.1 A number of different methods of destruction may be used for the destruction of sensitive material. The purpose of this section is to establish minimum standards that are acceptable to clients needs.	
7.2 Destruction by incineration is satisfactory for all paper waste, magnetic and optical data storage media, film and microfiche.	
7.3 The incineration process shall be carried out in an enclosed furnace with sufficient temperature and process to product a 100% ash result.	
7.4 The furnace used for incineration shall comply with Local Council, Labour and Health Department Regulations relating to the discharge of smoke and gases to the environment.	
7.5 Pulping is a satisfactory method of destruction of paper waste provided that residue is regularly inspected for the effectiveness of the destruction process.	
7.6 Both disintegration and shredding are acceptable methods for most types of sensitive material and are to be graded as per the following schedule:	

	Particle Cut		Straight Cut
Grade	Size mm^2	Max Width mm	Max Width mm
1	25	5	4
2	800	20	12
3	2000	40	20

DESCRIPTION	EVIDENCE
7.7 Hogging and shredding methods, which do not comply with the specifications listed in 11.6, are not secure destruction and therefore the process should be considered for upgrading and a Certification of Destruction should not be issued.	
7.8 Burial is not an acceptable form of destruction. If a client or company chooses to "securely" bury sensitive material then it is done outside of this Code of Practice. Compacting at the tip face excludes water and oxygen both of which are needed for bacteria to breakdown (and therefore) destroy material.	

SECTION 8: RECYCLING OF SENSITIVE MATERIAL

DESCRIPTION	EVIDENCE
8.1 Recycling of sensitive material is acceptable under the following criteria: a. All sensitive material must be destroyed to the standard set and agreed by the client prior to recycling b. Cartons, cardboard and other packaging may be recycled provided there is no client information on the packaging c. Plastics and non-ferrous metals may be recycled providing there is no client information displayed.	
8.2 Computer disks, magnetic tape or any other form of magnetic or optical data storage material shall not be recycled and must be destroyed by incineration, disintegration or shredding before disposal.	

SECTION 9: AUDIT

DESCRIPTION	EVIDENCE
9.1 In addition to any other external audit process the Client shall have the right to conduct an audit of the company's destruction process and building at any time during normal working hours. The cost of this audit to be met by the client.	

Auditor Signature: _____ Date: _____

For the Company:

Name: _____ Signature:_____ Date: _____

ANNEX ONE: DEFINITIONS

Client	*Any person or organisation supplying sensitive material or secure destruction*
Company	*Any person of persons who carry on business either individually or in partnership with any other person including a limited liability company, and who contract to supply a service for the destruction of sensitive material.*
Destruction	*The complete and irreversible physical erasure of the record which ensures that the record cannot be reconstituted or reconstructed.*
Destruction Officer	*Any person employed in the destruction of sensitive material*
Employer	*Any person or persons or company employing staff involved in the destruction of sensitive material*
PSPPI Act 2010	*The Private Security Personnel and Private Investigators Act 2010 and amendments*
Secure Destruction	*The complete and irreversible physical erasure of sensitive material which ensures that the material cannot be accessed, used, reconstituted or reconstructed by unauthorised persons.*
Security Destruction Facility	*Any facility where the actual secure destruction process is carried out*
Security Transport Officer	*Any person involved in the transportation of sensitive material destined for secure destruction*
Sensitive Material	*Any material or product conceived by the client to be of sensitive nature and that unauthorised access to, or use, or release of the material or product could cause harm or damage to the client.*
Sub Contractor	*Any person or company contracted to the company to provide either transportation or destruction of sensitive material.*

REFERENCES:

Legislation	*The Private Security Personnel and Private Investigators Act 2010 and amendments.*
Standards	*AS/NZS 1015:2011 Records management - Physical storage.*