GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

Approval of Secure Destruction Facilities

Information for Service Providers

June 2018

www.gcsb.govt.nz

New Zealand Government

Introduction

Secure destruction is a recognised practice in both the private and public sectors. It assists organisations in meeting legislative, regulatory and privacy requirements as well as forming part of good information assurance and governance practice. The NZISM and related policies require government agencies to securely destroy particular electronic equipment and media upon disposal in order to protect the data such equipment may contain.

Approved Facilities

The status of "approved facility" for the destruction of media and equipment may be granted by the Director-General GCSB under the NZISM. Approval depends upon the Director-General's satisfaction that the proposed facilities are capable of securely destroying IT equipment, devices and media to the standard required under the NZISM and related policies.

Approved facilities must demonstrate and adhere to agreed procedures, processes and performance monitoring to achieve secure destruction of equipment and media. Once approved to meet requirements for the destruction of highly classified items, facilities will automatically encompass all lower levels of classification.

Self-certification or assurance by prospective operators does not provide a level of assurance sufficient to meet the criteria of the NZISM. Detailed inspection and review by GCSB staff determines compliance with the required standards. It is important to note that an approval is NOT a certification or accreditation as described and defined in the NZISM.

Approvals are granted on a site-only basis and are not transferable between locations or organisations.

Approval Process

The overall approval process is summarized below:

1. A service provider (applicant) must first issue a written request to the GCSB for consideration as an Approved Secure Destruction Facility;
2. An initial meeting between the applicant and GCSB will then determine the logistics of the approval process and ensure common understanding of the requirements and conditions of approval;
3. A review of the proposed operation will take place, including:
    a. A physical site inspection;
    b. Examination of the applicant's documentation, workflows and procedures;
    c. Observation of the service provider's operations;
    d. An examination of the destruction equipment, including destruction of a sample and analysing the waste (integrity check);
4. If the applicant fails to meet the requirements of the PSR and NZISM, remedial actions will be required before the application can be processed further;
5. Failure to satisfactorily apply remedial measures may result in an application being declined;
6. On successfully meeting the requirements of the NZISM and PSR, the Director-General GCSB may grant the applicant approved status;
7. The applicant will be advised of this via a formal letter which will set out the approval, the security classifications of the media and equipment the facility may handle, and the time frame the approval applies for.

Approvals are typically issued for up three years, but may be of shorter duration. Approvals are also subject to ongoing inspections to ensure that facility operators continue to adhere the required conditions. Inspections will occur annually, but may also be more frequent at the discretion of the GCSB.

Service providers are required to advise the GCSB when major changes occur such as variations in equipment, process or ownership. Failure to do this or to meet required conditions of operation may result in a) requests for remediation measures to be applied to the facility, and / or b) revocation of any approval previously granted.

Initial requests

In any initial request to the GCSB Applicants should provide a covering letter and include following information:

Category	Detail
Contact Information	Organisation Legal Name
	Physical address of proposed facility
	Postal address
	Contact name, phone number, email address
Services Offered	Type of destruction
	Sensitive item transport
	Other destruction services (specify)
Types of items accepted	Electronic media (specify types)
	Motherboards, circuit boards
	Casings and frames
	Optical & other media
	Phones, radios, other portable devices
	Other (please specify)
Destruction Equipment	Manufacturer, type, capacity
	Conformation with any international destruction standards
	Provide a sample of output
Disposal Procedures	Metal recycling, component resale/export, shredder residue disposal, hazardous waste handling
Scope of application	Partial/single site/ multiple sites
	Limitations on destruction capability
	Limitations on disposal and recycling
Other information	Other accreditation or compliance held such as ISO, EPA licencing, waste export licences etc.
	Relevant industry association memberships.

Applications should be addressed to:

Manager, High Assurance Services Unit
Government Security Communications Bureau
Pipitea House on Pipitea,
1-15 Pipitea Street,
Pipitea,
Wellington 6011

Review materials

GCSB staff inspecting proposed secure destruction facilities will take the following topics into consideration.

Workflow and Procedure Documentation

Applicant's workflow and procedure documentation must include information and instructions relating to:

- Physical security and access control of the controlled destruction area;
- Collection, transport and receipt of materials for destruction;
- Destruction procedures;
- Personnel security requirements;
- Maintenance procedures and record keeping;
- Integrity Checks;
- Compromise procedures;
- Accommodation of visitors, inspectors and observers.

Workflow documentation should be aided by diagrams wherever appropriate.

Physical Site Inspection

Most destruction facilities will be treated as UNCLASSIFIED sites when **not** operating. Operators should, however, take sufficient precautions to safeguard the site and equipment from damage, interference or compromise. On this basis the following elements should be in place:

1. Destruction equipment must be installed within a controlled destruction area accessible only by authorised personnel. This will protect the equipment and also assist in meeting Health and Safety requirements for the operation of such equipment.
2. Controlled areas will typically be lockable, have video surveillance/CCTV and may also have intruder alarms installed.
3. When destruction equipment is installed, modified or decommissioned, such activities are recorded in engineering/maintenance records detailing:
    a. Date and time of action;
    b. Name and organisation of the person(s) performing the action;
    c. Any identifying serial numbers;
    d. Technical description of the installation or modification sufficient to allow later integrity checks.
4. Such records should be available for inspection as required.
5. Where changes to facility ownership, equipment or processes occur notification must be provided to the GCSB as soon as practicable.

Controlled Destruction Area

The controlled destruction area may be a portion or comprise the whole of the site of the external destruction facility. The secure destruction areas must have a secure perimeter such that unauthorised individuals without tools cannot gain access without drawing attention to themselves or activating any intrusion detection alarms.

Destruction equipment must be installed within a controlled destruction area, accessible only by authorised personnel. Access control, locks, video surveillance/CCTV and intruder alarms should be installed unless other compensating controls are in place, for example CCTV in the controlled area may be substituted by a facility-wide CCTV capability.

Temporary Holding Areas

Where items are stored in a holding area prior to destruction, the level of protection offered by the holding area must be at least equivalent to that provided by the controlled destruction area.

Separation of sensitive from non-sensitive items

Sensitive and security classified items that have been selected for destruction must be stored in a separate physical space from unclassified and / or non-sensitive items. This may be a separate room or holding container. Items received from different owners must be separated within the controlled destruction area.

Tracking

All items for destruction must be tracked through the destruction process by tracking individual items and any holding containers.

Holding Containers

Holding containers should be lockable, opaque and strong, preferably metal containers. Where sensitive or security classified items are stored in these containers, tamper-evident seals should be used and applied before transport.

Transport

The security classification of the media or devices to be destroyed will determine whether these can collected by the service provider or must be delivered by their owner. Containers holding sensitive and security classified items must be under observation at all times, until destruction is completed. Vehicles transporting materials must not be unattended at any time during transport.

Procedures must be established to deal with vehicle break-down or accident.

Timely Destruction

Items must be destroyed as soon as possible after arriving at the destruction facility and may not be stored overnight at such facilities.

External Supervision of Destruction

The destruction of certain security classified or sensitive materials must be witnessed by approved personnel from the agency owning these. This may be team of staff who are required to witness the entire procedure from transport to final destruction of the materials.

Service providers must accommodate this requirement for supervision and observation in their destruction procedures. Such supervisors and observers are NOT required to manage or handle any items or equipment themselves.

Destruction Procedure

Operating procedures should include:

- Destruction equipment must be operated by trained, authorised personnel only.
- For the destruction of sensitive or security classified material, destruction must be observed by authorised personnel from the customer agency unless written dispensations from the customer agency are in place.
- Appropriate provisions must be made for supervisors and observers. This extends to the delivery of any appropriate Health and Safety briefings, and any necessary safety equipment (hearing protection etc).
- All items received must be identified and recorded.
- Destruction of the items must be visually confirmed.
- A certificate of destruction recording serial numbers and any other identifying information must be provided on completion of the destruction process.
- The destruction equipment must be checked for any residue or unprocessed materials before shut-down;
- In the event of equipment failure before completion of the destruction, any residue and unprocessed items must be secured in a locked container.

Service Provider Personnel

All personnel with access to sensitive / security classified items or controlled destruction areas must sign a non-disclosure agreement stating that they will not disclose any protected information, customer details, scheduled destruction or collection and transport arrangements.

Maintenance Procedures and Record Keeping

Equipment and controlled destruction areas maintenance procedures must be documented in order to safeguard the security of the facility and equipment, as well as for equipment support and health and safety reasons.

Integrity Checks

The integrity of destruction equipment must be confirmed by an authorised person during installation, modification and thereafter at regular intervals, or in response to a security incident, to ensure that it has not been modified to facilitate an attack. Equipment must have a documented inspection schedule.

An Integrity Check should be undertaken:

1. Before approval to operate is granted;
2. After any major maintenance or machine modification or upgrade;
3. Where there is evidence of a site compromise or security breach.

The integrity check will:

1. Review any maintenance records;
2. Detail any parts of the equipment that could not be accessed;
3. Note any inconsistencies;
4. Process a sample through the equipment to validate particle size and completeness of destruction;
5. Visually confirm that the test items have been destroyed;
6. Ensure the residue (waste) from the processed sample meets specification.

Compromise procedures

Custodians must have documented procedures for identifying and recording suspected, potential, attempted or confirmed compromises of the sensitive items, including:

- Recording of all possible compromises, including where it was subsequently established that there was no compromise;
- For each possible compromise, recording details of time, location, personnel, sensitive items affected and precise circumstances;
- Recording of investigative and mitigating action considered and taken;
- Provision of verbal notification to the owner as
- soon as practicable;
- Provision of written notification to the owner as soon as practicable.

Disputes, Security Incidents, and Complaints

Any enquiries related to applications, disputes, security incidents or complaints can be directed to the GCSB care of:

Manager, High Assurance Services Unit
Government Security Communications Bureau
Pipitea House on Pipitea,
1-15 Pipitea Street,
Pipitea,
Wellington 6011

Key References

Document	Reference
New Zealand Information Security Manual (NZISM)	Chapter 12 – Product Security
	Chapter 13 – Media Management, Decommissioning and Disposal
	Section 12.6 – Product Sanitisation and Disposal
	Section 13.4 – Media Sanitisation
	Section 13.5 – Media Destruction

END OF DOCUMENT