GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

Approved Secure Destruction Facilities

Guidance to Agencies

June 2018

www.gcsb.govt.nz

New Zealand Government

Introduction

As technology has developed, it has become easier to recover information from IT equipment and media that may have been damaged, decommissioned or disposed of.

It has also become progressively more difficult to ensure that information is comprehensively deleted when sanitising media and equipment. If recovered, this information can be exploited by malicious actors, causing considerable damage to agencies and their interests.

Certain equipment and media must be destroyed at the end of its life. Residual and sometimes fragmented information can still be present, which creates a risk to official and security classified information. Critical factors include privacy concerns, legislative requirements to archive and protect official information, as well as obligations to protect security classified information.

Agencies need to follow a security process when decommissioning and disposing of IT equipment and media that has been used for official, sensitive or security classified information.

Approved Secure Destruction Facilities

As requirements have evolved, it has become less feasible for individual agencies to maintain specialist in-house destruction facilities for IT equipment and media. Nor are all commercial destruction services equipped or sufficiently secure for this service to be offered with acceptable levels of assurance.

The GCSB has instituted a process where an agency or commercial entity can apply to become an Approved Secure Destruction Facility. Approval from the Director-General GCSB provides assurance to the GCSB and agencies using the facility that equipment and media containing official, sensitive, and / or security classified information can be destroyed to the standard required by the NZISM.

A list of Approved Secure Destruction Facilities will be published on the GCSB website and added to as more facilities are approved.

Equipment that must be destroyed

Agencies must use an Approved Secure Destruction Facility to destroy equipment and storage media that cannot be safely sanitised. These may include:

- microfiche;
- microfilm;
- optical discs;
- printer ribbons and the impact surface facing the platen;
- programmable read-only memory (PROM, EPROM, EEPROM);
- flash memory and solid state or hybrid data storage devices;
- read-only memory; and
- faulty magnetic media that cannot be successfully sanitised.

See NZISM Chapter 13. Media Management, Decommissioning and Disposal for more information on sanitising and destruction. If you are unsure whether your equipment should be destroyed at an approved facility, please contact us at ISM@gcsb.govt.nz

Process and requirements

Agencies are responsible for making their own arrangements directly with the Approved Secure Destruction Facility.

It is up to agencies to ensure the arrangements align with their standing procurement and contract procedures.

The staff of the Approved Security Destruction Facility will operate the destruction machinery as they will have received the necessary technical and safety training. The sending agency is responsible for arranging transport, either directly delivering the items for destruction or arranging secure transport with the facility.

Transport of security classified IT equipment and media to any facility must also meet the requirements associated with that security classification. In some cases "safehand" requirements applying to CONFIDENTIAL, SECRET, TOP SECRET, and NZEO endorsed materials will apply. For further detail on transport requirements please refer to the PSR.

Agencies sending material to be destroyed will also need to schedule the timing of delivery and subsequent destruction in advance with the facility operators.

Escorting staff must remain with the security classified equipment and media at the Approved Secure Destruction Facility. This material **remains** security classified and must be escorted until it is destroyed. Destruction of the equipment and / or media must take place as soon as possible once it has arrived on site.

Approved Security Destruction Facilities are not permitted to store security classified materials. If for any reason a facility is unable to destroy the material, it will need to be transported back to the sending agency immediately. Agencies should be prepared for this eventuality.

Suitably cleared agency staff must observe destruction. Once it is complete and agency staff have verified that no material remains undestroyed, the facility operators must provide them with a certificate of destruction.

The certificate should be retained by the sending agency for audit purposes.

Disputes, Security Incidents, and Complaints

In the event of a dispute or complaint arising between an agency and an Approved Secure Destruction Facility, both parties should make every effort to resolve the matter.

Should this fail, or should security concerns about facility or agency operations arise, GCSB should be informed. This may in turn prompt the status of the destruction facility to be revised, and / or the involvement of the NZSIS as appropriate.

Enquiries related to disputes, security incidents and complaints can be directed to:

Manager, High Assurance Unit

Information Assurance and Cyber Directorate

Government Communications Security Bureau

Email: tech-liaision@gcsb.govt.nz