Te Puna Mātauranga o Aotearoa
NATIONAL LIBRARY OF NEW ZEALAND

National Library operating practice with regard to the security of electronic publications collected under the Legal Deposit provisions in the National Library of New Zealand (Te Puna Mātauranga o Aotearoa) Act 2003

Definitions

1. These definitions are used in this document:

Term/Abbreviation	Definition
The Act	National Library of New Zealand (Te Puna Mātauranga o Aotearoa) Act 2003
The Archive	National Digital Heritage Archive
DaaS	Desktop as a Service
The Department	Department of Internal Affairs
Electronic collections	Internet documents and offline documents collected by the Library in accordance with the provisions in the Act, and stored and managed in the National Digital Heritage Archive
Electronic publications	Any Internet document or offline document, as defined in the Act, collected in accordance with the provisions of the Act
IaaS	Infrastructure as a service In this document it refers to the New Zealand third party provider which manages the servers on which the Archive is hosted
Internet document	A public document that is published on the Internet, whether or not there is any restriction on access to the document; and includes the whole or part of a website
The Library	National Library of New Zealand
Offline document	An electronic document that is not an Internet document: examples include videotapes, CDs and DVDS, etc
PANZ	Publishers Association of New Zealand
TaaS	Telecommunications as a service

Introduction

2. The National Library is part of the Department of Internal Affairs. The Department has a duty of care to ensure that it maintains the integrity and security[1] of the information assets it stores and processes to deliver all the services for which it is responsible.
3. The provisions in the Act relating to deposit of electronic documents were activated on 11 August 2006 by the National Library Requirement (Electronic Documents) Notice 2006.
4. Electronic publications collected by the Library are held in the National Digital Heritage Archive, for long-term digital preservation. It uses the ExLibris Rosetta application. The system backend, including servers and physical storage is managed by an external supplier of Infrastructure as a Service to Government.
5. The Archive has been developed in accordance with best practice standards and guidelines for a trusted digital repository, and the Department is currently instituting an ongoing security roadmap for the Archive.
6. The Library recognises the importance of managing electronic publications securely, and the potential risks to a publisher's or other rights holder's interests if such publications are used in ways not permitted by the Act. In this undertaking, the Library makes a number of commitments to publishers for the secure management of electronic publications.

Commitment by the National Library

7. This statement is authorised by the National Librarian, and is effective from June 2016.
8. Amendments to this statement must be authorised by the National Librarian after consultation with the Publishers Association of New Zealand and any other interested parties.

Electronic Collections Security: Governance

9. The Department's information security policy and information security procedures apply to the Library's electronic collections.
10. Overall responsibility for electronic collections security is the responsibility of the National Librarian.
11. The Department's CIO has responsibility for the security of information in electronic form, including electronic collections of the Library. The Department has recently strengthened arrangements for security and privacy governance, including the creation of a Chief Security Officer role, in addition to the CIO role.
12. In addition to Departmental security governance processes, the Library will annually review its performance against the undertakings given in this statement. This review will be undertaken by the Chief Librarian, Alexander Turnbull Library and the Director, Content Services, and a report provided to the National Librarian. A copy will be made available to the President of PANZ.

Electronic Collections Security: processing and storing deposited material

13. The Library will manage any passwords or access credentials that are supplied by a publisher in accordance with section 33 of the Act in a secure repository and will ensure that these are only used by authorised personnel for the purposes permitted by the Act.
14. Electronic publications delivered to or copied by the Library in accordance with sections 31 (1) (b) and 31 (3) of the Act will be stored in secure systems including the Archive, to which only authorised personnel may have access for the purpose of processing deposited documents for storage and preservation.

---

[1] In accordance with New Zealand's Cyber Security Strategy https://www.dpmc.govt.nz/dpmc/publications/nzcss

15. The Library will store all deposited material, after processing, in the Archive, and once the deposited material has been ingested into the Archive, any copies that remain in processing systems outside of the Archive will be deleted.
16. The Department will maintain the Archive on a Virtual Private Network run over private circuits, protected by firewalls and intrusion detection and prevention systems, with no wider public internet access, and encrypting any communication between the firewalls for transferring data between the Library and the Archive at our IaaS provider.
17. The Department will ensure that its IaaS provider employs physical entry controls to ensure that only authorised personnel with an appropriate business need are permitted access to the secure areas hosting the Archive.
18. The Department's IaaS provider will implement policies to prevent such authorised personnel from making or disseminating unauthorised copies of deposited material stored in the Archive.
19. The Library will ensure that only authorised personnel with an appropriate business need are granted administrative access rights to the National Digital Heritage Archive, subject, where appropriate, to security checks before being granted such rights.
20. Any third party employed by the Library or the Department to acquire or process deposited material, or to carry out other permitted activities with deposited material, will be required to comply with policies and implement appropriate information security measures.
21. The Library will use best endeavours to prevent authorised personnel from making or disseminating unauthorised copies of deposited material.

Electronic Collections Security: using deposited material

22. The use of deposited material is specified in the Act:

> 34 Use of public documents in National Library
>
> (2) For the purposes of carrying out his or her duties, the National Librarian and any employee, contractor, or agent of the chief executive may possess, copy, store in electronic form (whether offline or online), and use any copy of a deposited document.
>
> (3) The National Librarian may provide not more than 3 copies of a deposited document for use by members of the public (whether at the premises of the National Library or elsewhere) but, except as provided in subsection (4) or with the publishers agreement, must not make the document available on the Internet.
>
> (4) If a deposited document is made publicly available on the Internet by the publisher without restriction on its access or use by members of the public, the National Librarian may make the document available for access and use by members of the public on the Internet (as well as in the manner permitted by subsection (3)).
>
> (5) Except as provided in subsections (2) to (4), the law relating to copyright applies to every deposited document.

23. The Library will use best endeavours to ensure that electronic publications are made available to the public only in accordance with section 34 of the Act.
24. Where a publisher has made an electronic publication available on the Internet with restriction on its access, the Library will implement systems and procedures to limit readers' concurrent access to no more than three copies at a time at the premises of the National Library, and it will not make the publication available on the Internet without the agreement of the publisher.

25. The Library will implement systems and procedures to ensure that no digital copies of Internet documents may be made by or for users, unless the rights holder has given written permission to do so or the deposited document was made publicly available on the Internet by the publisher without restriction on its access or use by members of the public.
26. Where a publisher has made an electronic publication available on the Internet without restriction on its use or access by members for the public, the Library may also make the publication available on the Internet without such restrictions.
27. Where a publisher has supplied offline documents, the Library will implement systems and procedures to limit readers' concurrent access to up to three copies at a time at the Library's premises or elsewhere.
28. The Library will implement systems and procedures to ensure copies of offline documents are supplied to users only in accordance with the Copyright Act 1994.

Electronic Collections Security: incidents and complaints

29. The Library will advise PANZ of a point of contact for any queries, complaints or incidents relating to the security of deposited material and this statement.
30. The Library will implement a formal process to manage and report any security incidents relating to deposited material and the commitments in this statement.
31. Any security incidents will be documented anonymously in the report to be provided to the National Librarian, with a copy supplied to the President of PANZ (see point 12 above).

Audits and Assurance

32. The Department has a programme of internal and external IT security audits of its infrastructure, including the National Digital Heritage Archive.
33. All assets supporting the NDHA including the Iaas, TaaS and the DaaS provisions are considered 'HighRisk/High Value' assets by the Department and therefore have Security and Risk Assessment roadmaps. They require their Certification and Accreditation to be valid at all times.
34. Certification and Accreditation is a fundamental governance and assurance process used by all New Zealand Government Departments and designed to provide confidence to all stakeholders that information and its associated technology are well-managed, that risks are properly identified and mitigated and that governance responsibilities can demonstrably be met. It is deemed essential for credible and effective information assurance governance.

June 2016

Acknowledgement: In creating this document the National Library of New Zealand would like to acknowledge the permission of the British Library to use their document: *Undertaking to the Joint Committee on Legal Deposit on the Security of deposited non-print publications, 2013*.