"…For the purposes of the FOI Act, please reply with a copy of your agency's documents showing: · information backup and archiving policies (or such documents showing how often dochub, content manager, outlook and any other resources of your agency are backed up, how many copies of the backups are made, and for how long the backups are kept) · (1) outlook (i.e. email), (2) content manager and (3) dochub information that is (A) initially recorded and (B) ultimately backed up

1. The department's standard backup approach is to backup every 24 hours and retain for 30 days.
    a. This is outlined in the ICT Backup and Recovery Policy. This policy is outdated and incorrectly notes a 90 day retention period.
    b. Two copies of backups are kept for redundancy purposes.
2. On archiving we take this to mean the moving of information to a separate storage location and as such is covered under the backup points (above).
    a. Regarding specific reference to the DocHub and Content Manager, the department applies records authorities to the records in these systems, which are publicly available on the National Archives of Australia website.
        i. General Records Authorities - https://www.naa.gov.au/information-management/records-authorities/types-records-authorities#general-ra
        ii. Agency specific Records Authorities - https://www.naa.gov.au/information-management/records-authorities/agency-specific-records-authorities

(this should show the types of user actions, such as searches, file manipulations, deletions etc - if this level of detail is not documented in word/pdf format, it may be obtained by your IT engineers from system configuration files instead) There is no need to include personal, duplicate or public information (but please do point me to any relevant public information, if it exists)."

The department's standard logging approach is to collect event logs immediately where they are backed-up every 24 hours retained as per the Australian Signals Directorate Information Security Manual requirements - https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism.

Department of Industry, Innovation and Science

ICT Backup and Recovery Policy

Version 0.1 | 19 June 2019

Document Administration

Document Information

File Name	Document Logical Location
DIIS ICT Backup and Recovery Policy	s47E(d)

Associated Documents

File Name	Document Logical Location
s4E(d)	
ASD Essential 8	https://www.cyber.gov.au/publications/essential-eight-explained

Change History

Version	Date	Description	Created by
0.1	19/06/2019	Initial draft	s22
0.2	06/07/2019	Feedback accepted, updated RPO and RTO	s22
0.3	30/07/2019	Feedback accepted	s22

Consultation

Version	Date	Description
0.1	19/06/2019	s47E(d)
0.1	19/06/2019	s47E(d)
0.1	06/07/2019	s22 s47E(d)

Approval

Version	Date	Approver
1.0	s47E(d)	s22 s47E(d)

Table of Contents

DOCUMENT ADMINISTRATION **2**

DOCUMENT INFORMATION 2
ASSOCIATED DOCUMENTS 2
CHANGE HISTORY 2
CONSULTATION 2
APPROVAL 2

PURPOSE **4**

AUDIENCE **4**

RELATED DOCUMENTS **4**

ADMINISTRATION OF POLICY **4**

PRINCIPLES **5**

ESSENTIAL EIGHT MATURITY MODEL **5**

BACKUP REQUIREMENTS/FREQUENCY **6**

ICT SYSTEM CLASS FRAMEWORK **6**

BACKUP RETENTION **6**

RESTORATION PROCEDURES & DOCUMENTATION **8**

BACKUP STORAGE **8**

RESPONSIBILITY **8**

Purpose

The purpose of this document is to define the objectives, accountabilities and application of the Departments backup, recovery and retention policy. This policy outlines the standards for backup and retention required to provide adequate data protection for the Department's data and ICT systems.

Audience

This document is intended as a design artefact and should be read by stakeholders including:

s47E(d)

Related Documents

This document should be read in conjunction with the documents/links listed below.

- Australian Signals Directorate's Australian Cyber Security Centre (ACSC) - Essential Eight Maturity Model
    - Australian Signals Directorate's - Essential Eight Maturity Model

s47E(d)

- Australian Government Information Security Manual (ISM)
    - https://www.cyber.gov.au/ism

Administration of Policy

s47E(d)

Principles

The following principles direct this policy:

- Data protection and backup capabilities must provide a level of assurance and cover that allows the Department to achieve its objectives efficiently and provide adequate risk mitigation;

s47E(d)

- Backup and recovery systems are to be used for the purposes of recovering data or ICT systems due to a disaster event (DR), data corruption, accidental deletion, an unplanned system outage from which the system can't be recovered through other means, a malicious attack (internal or external) or a failed system upgrade.

s47E(d)

- Data protection and backup of the Department's data assets that are hosted outside of the Department's ICT infrastructure (e.g. in business systems that are managed by external service providers) must comply with the standards defined in this policy. Contracts with such external hosted service providers must include compliance with this policy.

Essential Eight Maturity Model

The Department will adhere to the ASD's essential eight maturity model enabling the Department to achieve and maintain maturity level three for data protection. To achieve this the Department will ensure:

- Backups of important information, software and configuration settings are performed at least daily.
- Backups are stored offline, or online but in a non-rewritable and non-erasable manner.
- Backups are stored for three months or greater.
- Full back up and restoration processes are tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur s47E(d)

- Partial backup and restoration processes are tested on an annual or more frequent basis.

Backup Requirements/Frequency

s47E(d)
s47E(d)

The following outlines the Departments backup requirements and frequency:

- Production data and ICT systems will be protected by daily backups. The default backup frequency will be once every 24 hours for production data and ICT systems.

s47E(d)

ICT System Class Framework – Extract as of 30/07/2019

s47E(d)

Backup Retention

The Department's data protection systems are the authoritative source of truth for which data and systems are backed up, how often these are backed up and what retention periods are in place for backup sets. The following outlines the Departments baseline ICT Backup and Retention policy:

Production

- The default retention period for production backup sets and copies is 90 days this will be achieved by ensuring weekly full backups are kept for 90 days and incremental backups are kept for 30 days.

s47E(d)

- At least two copies of a backup will be taken and stored.

s47E(d)

s47E(d)

Restoration Procedures & Documentation

s47E(d)

Backup Storage

s47E(d)

Responsibility

s47E(d)

1. The department's standard backup approach is to backup every 24 hours and retain for 30 days.
    a. This is outlined in the ICT Backup and Recovery Policy. This policy is outdated and incorrectly notes a 90 day retention period.
    b. Two copies of backups are kept for redundancy purposes.
2. On archiving we take this to mean the moving of information to a separate storage location and as such is covered under the backup points (above).
    a. Regarding specific reference to the DocHub and Content Manager, the department applies records authorities to the records in these systems, which are publicly available on the National Archives of Australia website.
        i. General Records Authorities - https://www.naa.gov.au/information-management/records-authorities/types-records-authorities#general-ra
        ii. Agency specific Records Authorities - https://www.naa.gov.au/information-management/records-authorities/agency-specific-records-authorities

The department's standard logging approach is to collect event logs immediately where they are backed-up every 24 hours retained as per the Australian Signals Directorate Information Security Manual requirements - https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism.