Backup & Data Retention Policy

On this Page

Title	Backup & Data Retention Policy
Subject	Security
Classification	INTERNAL USE
Audience	All staff
Status	CURRENT
Prepared By	Michael Wicks
Prepared Date	04 May 2021
Reviewed By	Tony Wilson
Reviewed Date	14 Jun 2023
Approved By	Alan Ariti
Approved Date	15 Jun 2023
Effective Date of Policy Version	28 Feb 2023
Version	v. 34
Next Review Date	

THE WHY

1. Purpose

1.1 The purpose of this policy is to:

1.1.1 Ensure that there is a defined, consistent and reliable process for recovering Vocus information systems and data.

1.1.2 Set out Vocus policy regarding the retention, archiving and destruction of Vocus data.

2. Objectives

2.1 The objectives of this Policy are to:

2.1.1 Define the requirements for the backup and recovery of Vocus information systems and data.

2.1.2 Define backup standards according to data type.

2.1.3 Prevent the loss of data arising from accidental deletion, corruption, system failure, or disaster.

2.1.4 Document Vocus' data retention requirements.

2.1.5 Enable Vocus to meet its regulatory, legal, contractual and operational responsibilities in all jurisdictions.

2.1.6 Balance the need to reduce the impact on resources and costs of retaining data.

THE WHAT

3. Scope

3.1 This policy applies to all personnel and all data held in respect of current and former customers and business activities of Vocus.

4. Definitions

Term	Definition
Business Data	Data used for day-to-day operations, the retention periods for which are dependent upon the requirements of their specific use. Any Business Data that qualifies as Required Data is classified and treated as Required Data and shall be retained accordingly. For example, internal phone and email records, help desk statistics, marketing and demographic information.
Backup Frequency	The timeframe for how often backups occur.
Backup Retention Period	The amount of time data should be retained.
Configuration	The group of settings that controls, flow and operate to support the network communication of an organisation.
Differential Backup	Data is copied in its entirety to begin with, and then only new or updated data is backed up during subsequent backup events.
Full Backup	Data is copied in its entirety.
Image	A logical copy/snapshot of volume content, captured at a particular point in time.

Incremental Backup	Data is copied in its entirety to begin with, and then only sets of backups with a change are backed up during subsequent backup events.
Information System	A major application or general support system for storing, processing or transmitting Vocus information.
Information System Owner	The individual or business unit assigned responsibility for an Information System (including its procurement, development, integration, modification, operation, and/or maintenance and disposal).
Required Data	Data that shall be retained for defined periods to meet regulatory, legal, contractual or operational obligations. For example, accounting records, customer information for law enforcement requests, contractual obligations.
Recovery Point Objective (RPO)	The interval of time that might pass during a disruption before the quantity of data lost during that period exceeds the Business Continuity Plan's maximum allowable threshold.
Recovery Time Objective (RTO)	The amount of real time a business has to restore its processes at an acceptable service level after a disaster to avoid intolerable consequences associated with the disruption.

THE HOW

5. Requirements

5.1 Information system resources shall be backed-up at scheduled intervals to provide assurance of restoration in the event of loss or corruption of data and for business continuity purposes as required.

5.2 Information backed up shall be retained in accordance with the Schedule A - Backup & Data Retention Timeframes.

5.3 Procedures shall be in place to ensure a successful recovery of information systems and information.

5.4 All archival backup records stored offsite are to be recorded to reflect the date when the data was most recently modified together with the nature of the data. This is to facilitate the determination if certain data is held in archival storage.

5.5 A directory of the files and their locations will be generated, either automatically or manually.

5.6 Build documentation

5.6.1 The Project and Information System Owner implementing or managing a Information System shall document processes and test recovery routines to mitigate risks of data loss.

5.6.2 The Systems and Infrastructure Team is responsible for backing up systems and information in accordance with the documented processes and test recovery routines.

5.7 Data Backup

5.7.1 Production Systems data shall always be backed on a regular agreed interval.

5.7.2 Backup frequency for UAT or Staging environments shall be at the discretion of the Information System Owner.

5.7.3 Requirements for additional systems to be included in backup schedules shall be setup by project or the person delivering the system into Production.

5.8 Image and Configuration Backups

5.8.1 Backups of Information Systems (Software, Operating System, Server, Network Configuration) shall be taken and stored to provide for rapid restoration to a known good state, including:

- Image backups
- Configuration backups

5.8.2 Images shall not be used for routine backups.
5.8.3 The Business Continuity requirements mandated by RTO and RPO determine the retention time for Image and Configuration backups.

5.9 Backup review

5.9.1 Backup logs (including backup failures) shall be reviewed. Backup review frequency shall be based on criticality of the data type to delivery of business objectives and legislative obligations.

5.9.2 Tests shall be conducted to investigate the cause of backup failures, and action taken to prevent recurrence.

5.10 Backup Timeframes

5.10.1 Backups will be timed for minimal impact on the production environment.

5.10.2 Backup timeframes shall be based on criticality of the data type to delivery of business objectives and legislative obligations.

5.10.3 Backups are scheduled as one of the following:

i. Daily
ii. Weekly
iii. Monthly
iv. Annual
v. Archive
vi. Once-off

5.10.4 According to standard definitions of terms, backups are determined as:

i. Full
ii. Differential
iii. Incremental

5.10.5 Systems and Infrastructure Team backup services will be performed in accordance with Schedule A - Backup & Data Retention Timeframes.

5.11 Storage

5.11.1 Backup data should comply with the following:

5.11.1.1 Be retained on a disk (no data on tapes or other external media) that is separate to the disk on which the original data is stored.

5.11.1.2 Backup solutions shall be automated.

5.11.1.3 Be synchronised across multiple sites.

5.11.2 The storage requirements shall be based on criticality of the data type to delivery of business objectives and legislative obligations.

5.11.3 Data is to be maintained on central accessible storage media and not in personal archives on desktops and local media.

5.12 Backup Restorations

5.12.1 Restoration tests will be conducted by the Systems and Infrastructure Team at regular intervals.

5.12.2 Requests for restoration of Information Systems and data shall be logged with IT Support.

5.12.3 When performing a restoration to a live system take a backup prior to proceeding.

5.12.4 Users will be notified of the outcome of the restore.

6. Exceptions

6.1 If an exception from this policy is required, a formal request shall be made by the Information System Owner to the Chief Information Security Officer and General Manager Technology Operations or their delegate for further security risk assessment in accordance with the Information Security Exception Procedure.

6.2 Upon any exception being granted, a risk shall be recorded by the Information Systems Owner in the Technology Risk Register under this Policy name.

THE WHO

7. Responsibility

7.1 Vocus will be accountable for the loss of Required Data and Business Data within defined retention periods.

7.2 General Managers - have responsibility to ensure all data for their business unit is backed up and retained in accordance with this Policy. This responsibility extends to ensuring that Systems and Infrastructure Team have adequate knowledge of the retention requirements.

7.3 Legal Team - have responsibility to provide effective advice regarding legal data retention requirements pursuant to maintaining Schedule A - Backup & Data Retention Timeframes.

7.4 Systems and Infrastructure Team - have responsibility for backup and data retention in accordance with Schedule A - Backup & Data Retention Timeframes.

7.5 All users - Each user of any computer system or software program is individually responsible for retaining or deleting electronic data in accordance with this policy.

THE DETAIL

8. Non-compliance

8.1 Vocus will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, logging and monitoring, and feedback to the policy owner.

8.2 Failure to comply with the requirements of this policy may result in disciplinary action in accordance with Vocus' disciplinary process.

9. Supporting Information

- Information Classification and Handling Policy

Schedule A - Backup & Data Retention Timeframes

- The Systems and Infrastructure Team runs Incremental Backups daily and Full Backups once per week.

Data Type	Data Examples	Data Notes	Data Retention Period

Specified User Accounts	Executive Management, General Managers, Financial Controllers, Legal Counsel, Secretarial and others nominated by these functions.	From the termination date. Includes unstructured data such as file shares and email.	7 Years
	All other employees		6 months
Financial Records	Invoices, receipts, orders for the payment of money, bills of exchange, cheques, promissory notes, vouchers and other documents of prime entry; and such working papers and other documents as are necessary to explain the methods and calculations by which accounts are made up that correctly record and explain the transactions and including any transactions as trustee) and would enable true and fair financial statements to be prepared.	After the completion of the transactions to which they relate	7 Years
Tax Records	Income Tax Assessment, Documents relevant to income and expenditure, and documents containing particulars of any election, estimate, determination or calculation Capital Gains Tax and GST requirements	Or the end of the assessment period if so extended by a Tax Commissioner, whichever is the later.	7 Years
Employee Records	Records relating to employees and pay slips including name, date of birth, classification, full-time, or part time, permanent, temporary or casual, date employment began, records of start and finishing times and total hours worked, pay details, leave details, superannuation contributions.	After employment is terminated.	7 Years
Call Recordings	Call recordings containing verbal contracts	From date of creation	6 Years
Customer Records	Details relating to customer accounts such as name, contact details, services provisioned	After last billed date	3 Years

Telecommunications records: data set - the subscriber of accounts, services, telco devices and other relevant services - the source of communication - the destination of communication - date, time, duration of communication - type of communication of a relevant service the location of equipment or line used in connection with a communication	Those telecommunications records required to be retained by law. **s187AA** – **Information to be kept**: must keep the data set encrypted and protected from unauthorised interference and access for the life of the account. When an account is closed, a smaller data set (set out in item 1, column 2 (a),(b) of the data set) must be retained for a further 2 years after the account is closed. **s187C – Period for keeping information and documents:** The general period for which a service provider must keep or cause to be kept information or document under section 187A is: - starting when the information came into existence, and - ending **2 years** after the closure of the account to which the information relates/ came into existence. - s187C (3) – this section does not prevent a service provider from keeping information/documents for a period that is longer than what is prescribed here. [Note: the data retained for these purposes is retained in a dedicated data warehouse and accessed via Swordfish when responding to requests for data from law enforcement/security agencies] refer to Data Hygiene Policy for further information - Data Hygiene Policy	Australian Data Retention Act Records maintained for two years after closure of account. Some subscriber data (such as information relating to the subscriber and the services/device provided) needs to be retained for two years after closure of the account. refer to Data Hygiene Policy for further information - Data Hygiene Policy	2 years
Audit logs	Logs of user activity and system access	From creation date	1 Year
Partners, agents and third party accounts	Records relating to third parties which access Vocus systems	After termination of account	6 Months
Credit Card cardholder records	Credit card account numbers are not to be stored on Vocus systems other than in tokenised form. Authentication data such as verification pins are not to be stored. Card account numbers stored on PCI compliant 3rd party systems must only be kept for the minimum time required such as when the account is active.	After the last bill date and account close.	30 Days
Default	Data which does not fall under the requirements above, including data required to be retained for a shorter period than 2 years.	This includes unstructured data such as file shares and email excluding specified accounts listed above.	2 Years maximum