2Cana Policy for Backups and Recovery			
ISSUED BY	Systems Team	Date	2019/06/13
APPROVED BY	Management Forum		

Revision History

Date	Author	Details
2019/06/13	Raymond Diack	Original

Purpose

This Policy is approved by 2Cana Risk Management and sets out the Backups and Recovery Policy within the company. The purpose of this policy is to define standards to be met by all backup systems operated by the 2Cana Systems Team. These standards are designed to minimise the potential exposure to 2Cana Solutions from the loss of sensitive or company confidential data, intellectual property, damage to public image etc., which may follow from unauthorised use of 2Cana company resources.

Policy Scope

This policy applies to all employees of 2Cana Solutions responsible for administering backups, as well as Vendors, Contractors, 3rd Parties and any others involved with 2Cana Solutions in terms of backups and recovery. All backup systems operated by 2Cana Solutions must comply with this policy.

Violation and Enforcement of Policy

If it is suspected that this policy is not being followed, report the incident to the Head of 2Cana Systems and IT Risk Management. Any exceptions to this policy must be approved in advance by the Head of 2Cana Systems and IT Risk Management. Any person found to have violated this policy will be subject to appropriate disciplinary action as defined by the provisions of the Company.

Ownership and Responsibility

Backup systems within the scope of this policy are administered by the 2Cana Systems Team, who are responsible for the following:

- Equipment must be documented and monitored daily, using both automated and manual monitoring (daily checks) as appropriate.
- This policy must always be adhered to, in terms of ongoing administration of backup systems as well as implementation of new systems.
- Changes to existing backup systems and deployment of new systems must follow the 2Cana Solutions change management processes and procedures.

Backup Configuration

- All changing data of value must be backed up daily. Daily backups may be incremental.
- Data of a static nature which changes very infrequently may be backed up weekly.
- Full backups must be run weekly and monthly.
- Backup selection lists must be configured with oversight and input from the team involved with administering that system.
- Backups of database systems must be coordinated with the DBAs responsible for those systems. The database vendor's own backup software is often the safest choice for application-aware backups. For Oracle systems, RMAN backups are written to disk and then backed up to tape. For Microsoft SQL systems, SQL Maintenance Plans write backups to disk and we then back these up to tape. Timing must be considered to ensure that the backup server only initiates a backup job to tape once the backup to disk is complete by the relevant DBMS, to ensure backup consistency.
- Granular backups are run where appropriate to allow single-object recovery.
- Backup selection lists are reviewed when any changes are made to the selection lists, or whenever new servers are deployed.
- All backups to removable media must be encrypted using industry-standard encryption. The encryption keys must be stored in a safe location and must only be accessible to staff responsible for administering the backup environment. Note that encryption was introduced in 2019/02, and thus tapes rotated on a monthly basis will only all be encrypted in 2020/02. As a mitigating control, note that these tapes are stored at a secure facility.

Monitoring

Backup jobs should be monitored daily by the desktop team and reported on via Daily Checks reports. Any failures should be reported through to the wider Systems Team for investigation. If corrective action can immediately be taken, or if the there is no clear cause for the failure, the job should be re-run. The goal should always be for all backups to complete with success on every run. If there are major problems and there is not enough time to complete all failed backups, priority should be given to jobs that have a longer retention period i.e. Monthly/Weekly jobs over Daily jobs.

Media Storage and Handling

- Tape media should be rotated offsite daily and stored securely. Tapes should only be handled by authorized personnel.
- Every effort should be taken to take nightly tapes offsite the following day. If backups overrun for whatever reason, the tapes may be kept onsite to allow completion, but must be sent offsite the following day with return dates carefully set as appropriate. Return dates are set for the day before the tapes are needed, to ensure that any errors in tape handling can be easily corrected in time for backups to run.
- Tapes requested from offsite storage for restores must be returned to offsite storage with the original return date specified.
- Once a month, the receipts from the offsite storage service provider should be examined by the desktop team and compared against the monthly media used report using a sample of tapes to verify that tapes are indeed being sent offsite.
- Media set data retention periods:
    - Daily – 2 weeks
    - Weekly – 8 weeks
    - Monthly – 12 months
- Faulty and retired tapes are destroyed.

Patching and Maintenance

Installing up-to-date vendor patches is critical for the security and reliability of the system, and to unlock new functionality. Backup server software should be upgraded within 6 months of release, unless there is a compelling reason not to do so. When the backup server software is upgraded, all Agents should be upgraded as soon as possible thereafter. The patching of the host server should be done in accordance with the general server patching policy. However, special treatment needs to be given to backup systems since they cannot be rebooted automatically at night as there may be backups in progress. Patches are therefore installed during business hours once backups have completed and the system is idle.

Physical Access

Physical access to the backup servers must be restricted to authorized personnel only through appropriate access control systems. In a hosting environment, the cabinet must be kept locked unless authorized work is in progress. In the on-premises server room, the server room door must be kept locked unless authorized work is in progress.

Recovery Testing

Recovery of backups should be completed every quarter. If a restore needs to be done, this can be considered a recovery test for that quarter. A log of recovery tests should be maintained. Once a year, a DR test should be conducted for each client database. The client will be given the option to get involved with testing.

Change Management

A Change Management process is critical, ensuring that changes are made in a logical, orderly manner. Individuals responsible for administering backup systems must always adhere to the 2Cana Change Management process.