Office of the Chief Information Officer (OoCIO)
National Backup and Restore Policy

Proposal Title	National Backup and Restore Policy
Project Sponsor	James Carroll
Proposer	Nicky Power
Division	Name
Portfolio	Name
Programme	Name
Status	☐ Draft ☐ Complete, Awaiting approval ☒ Approved
Version Date	21/11/2019

Purpose and scope

To establish a National Standard for backup and recovery that includes backup system policies, Recovery Point Objective (RPO), retention periods, monitoring, testing, roles, and responsibilities.

This Standard policy is only applicable when the Recovery Point Objective (RPO) is 24 hours or more. If the requirement is a more demanding RPO, the business must implement a High Availability solution.

With the unprecedented growth of data volumes, OoCIO must provide a consistent and efficient approach to Backup & Recovery element of Data Management.

Which provides the following:

Backup and Recovery to protect data in the organisation in the event of

- Equipment failure
- Intentional destruction of data
- Data Corruption or Disaster Recovery.

eDiscovery

eDiscovery is a specific service provided to the Freedom of Information (FOI) team or Legal teams where they can request information to be recovered. This information needs to be identified by keyword or email message(s).

The Backup and Recovery policy must align with Business Continuity / Disaster Recovery plans of the HSE.

Audience

The audience for this document OoCIO and HSE business owners.

Information Classification Policy

The Information Classification Policy outlines four classes of information generated by the HSE. While the Information Security Policy outlines that controls must be in place to preserve the confidentiality, availability and integrity of its information.

http://hsenet.hse.ie/OoCIO/Service_Management/PoliciesProcedures/Policies/HSE_Information_Classification_Handling_Policy.pdf

The Business needs to classify the data as per policy and verify the backup option is appropriate. As the Backup and Recovery service itself is not aware of the information classification of the data been backed up, all backups are considered to be classified as **Internal Information**.

Datatypes and their backup methodology

This policy discusses the backup methodology for each datatype outlined below.

Electronic Files:

All files stored on the servers must be included in the backup schedule of that server. This includes operating system files and user generated files.

Email:

All emails at mailbox level (send & receive) via the HSE email system are backed up. Emails that reside on a client which have not been synchronised to the email server, are not included in the backup

Servers:

Virtual and Physical Servers: Backup and Recovery service provides backup via agent or snapshot for the following operating systems: Windows 2003 Server and above, and Linux supported kernel.
Citrix Servers: Backup and Recovery service provides backups of these servers via snapshots.
Database Servers: Backup and Recovery Service provides backup of the server itself via an agent, the database itself is backed up by the DBA.

Databases:

The Database Administrator (Application DBA can be either HSE or 3rd party) is responsible for backing up the databases to a location provided by the Backup and Recovery Service. The Backup and Recovery Service is only responsible for backing up the database backup file prepared by the DBA in that location.

Microsoft SQL: Database is backed up via a Database maintenance job

Oracle: Database is backed up via the RMAN (Recovery Manager) tool

MYSQL: Database is backed up via a script or tool

Active Directory:

Backup and Recovery service provides backup of AD following the Microsoft recommended procedure.

Office 365:

Backups are presently out of scope for the Backup and Recovery service.

Azure Services:

Backups are presently out of scope for the Backup and Recovery service.

Out of scope:

Not all data of a recognized datatype is supported by the Backup and Recovery Service. Explicitly, the following data is out of scope, no matter which datatype they are:

- Physical Data, stored on paper, USB devices, CDs etc
- Data that is not stored in an HSE Tier 1 (National) or Tier 2 (Regional) data centre
- Data that is stored on a end user device (Desktop, Laptop & Tablets)
- Data stored on mobile phone device
- Data in Transit (Protection responsibility of the Transport Layer)
- Data in memory / cache / swap files

Data Centre:

There are 3 tiers defined for Data centres:

- Tier 1: - National data centre: the target used for all backups is Disk to Disk to Tape (Tiered storage). Backup data stored is written to tape on a monthly basis. Tapes are stored off site in an approved facility.
- Tier 2: - Regional server room: the target used for all backups is Disk to Disk to Tape (Tiered storage). Backup data stored is written to tape on a monthly basis. Tapes are removed from Tape Library by approved staff and stored in a fire proof safe. The safe must be located in a secure location where unauthorised access is prohibited
- Tier 3: - Non-standard room where server(s) are in operation. This is not a data centre.

Backup software:

- Tier 1 & Tier 2: - An enterprise software solution must be deployed at these facilities.
- Tier 3: -: It is expected that the policy as outlined will be followed.

Backup Schedules & Retention

The following backup schedules outlined below:

- Daily incremental:
    - Runs every 24 hours.
    - Backup to a backup target in the same location and synchronised with a remote backup target.
    - Retention of 3 months on local and remote backup targets.

- Monthly Full:
    - Runs on the last Friday of the Month
    - Backup to a backup target at the same location which is synchronised to a remote backup target. This remote target is consequently archived to tape.
    - Retention of 3 months on local and remote backup targets.
    - Retention of 7 years backup data on tape.

Exceptions:

- Database Servers follow the Monthly Full schedule only. The databases on those servers can follow both schedules when backed up to a separate location, as described at the Databases datatype.
- Citrix and Virtual App Servers follow the Monthly Full schedule only.
- Training, Test and Development Servers follow the Monthly Full schedule only.

Schedule for server types are outlined below. The backup schedule for a server must be determine business owner

Backup Schedule				
Server Types	**Daily (Incremental)**	**Weekly (Full)**	**Monthly Full**	**Example**
Electronic files (File Server)	Yes	Yes	Yes	File Shares: - Files are modified on a daily basis then daily backups must be performed
E-Mail	Yes	Yes	Yes	Exchange / Notes Servers change on a regular basis then daily backups must be performed
Virtual or Physical Server (Static)			Yes	Web, Citrix, Business Application servers: - these servers do not store files which are updated then monthly backups must be performed.
Virtual or Physical Server (Dynamic)	Yes	Yes	Yes	Proxy, DNS, DCHP, Business applications Servers: - these servers store files which are updated frequently then daily backups must be performed
Database – Microsoft SQL	Yes (full)		Yes	The database administrator must complete a backup of the database (daily) and transaction logs. The Server backup does not include the database.
Database –ORACLE	Yes		Yes	The database administrator must back up the database using the RMAN (Recovery Manager) tool. Daily backups must be performed
Database – MYSQL	Yes		Yes	The database administrator must back up the database using a script or tool. Daily backups must be performed
Active Directory	Yes	Yes	Yes	Daily backups must be performed.

Service Requests

Backup request

Business owners and project managers must ensure their solutions have a backup and recovery service in place before moving to production

Restore request

Any restore required must be submitted to the relevant Service Desk. The requestor must provide the restore details such as server name, the full location of the data type and date of the data type to be restored. The requestor must receive an automated email with a summary and ticket reference.

eDiscovery request

An eDiscovery request must be submitted by the FOI or Legal teams. The requestor must provide details of the search criteria such as a specific name of a person or keyword and timelines such as date.

The search criteria determine if the operation is handled either internally or externally.

- If the eDiscovery operation is handled internally, the requestor must receive a timeline for recovery. Once the timeline is accepted by the requestor, the Backup and Recovery Service is authorised to recover the user information. It is then the responsibility of the requestor to search and filter for the required information from the recovered data.
- If the eDiscovery operation is handled by an external resource, the Backup and Recovery Service must provide the costs of the recovery to the requestor. Upon approval by the requestor, the information must be restored by the external resource and handed over to the requestor.

All communication between the requestor and other parties involved (internally or externally) must be recorded.

Roles and Responsibilities

Business Manager – Business stakeholder responsible for the day-to-day operation of the service

Business Owner – Person who will be accountable to the business for the operation of the service

OoCIO Project Manager – Decision Maker.

It is the Business Owner & Project managers role and responsibility to provide:

- Recovery Time Objective (RTO)
- Recovery Point Objective (RPO)

Backup Administrator - must adhere to the Backup and Restore policy and adhere to the agreed business RPO & RTO.

Service Reporting

The following reports must be made available. These reports allow business owners and project managers to view the status of the backups of their data.

Business Owner and Project Managers

- Backup Success Rate (Daily, Weekly, Monthly and Yearly)
- Backup Failure Rate (Daily, Weekly, Monthly and Yearly)

Internal Only (Technology Dept)

- Backup Disk Capacity
- Recovery Readiness
- Data growth on back up
- Any Backups jobs modified

Tape Management

Backup Tape

Removable media (tape) must be uniquely identified by a barcode.

There should be no hand-written stickers or notes attached to a tape.

- Tapes must be stored in a locked secure area.
- Removable media must be stored in a temperature and humidity-controlled environment.
- Handling of Tapes:
    - Removable media (tape) must be placed in protective container when being stored or transported

Storage of Backups

Backups must be stored onsite (in a locked secure area) or offsite at an Irish Government Storage Facility or in an approved Third Party Storage facility.

– Onsite Storage of Backups: See HSE Information Technology Acceptable Use Policy, § 4.15.1
– Offsite Storage of Backups-Irish Government Storage Facilities: See HSE Information Technology Acceptable Use Policy, § 4.15.3
– Offsite Storage of Backups-Third Party Storage Facilities: See HSE Information Technology Acceptable Use Policy, § 4.15.4

Link: HSE Information Technology Acceptable Usage Policy

Security

Encryption

Backup Tapes must not be encrypted.

Encrypting tapes may prevent any data recovery in the future. Backup Products come to an end of life or may not be fit for purpose; if encryption has been set enabled, data cannot be recovered by a different product.

Appendix

A. Document References

HSE IT Security Policy:
hsenet.hse.ie/OoCIO/Service_Management/PoliciesProcedures/Policies/HSE_I_T_Security_Policy.pdf

HSE IT Acceptable Use Policy:
http://hsenet.hse.ie/OoCIO/Service_Management/PoliciesProcedures/Policies/HSE_I_T_Acceptable_Use_Policy.pdf

B. Definitions

Restore - The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.

Retention – The length of time backup media and catalogue must be maintained, available for a restore.

Backup Object – The unit of data being backed up. Examples of a backup object: Virtual Machine, SQL database, a file server volume, System State

MTR (Maximum Time Recovery) is the total time to recover a system or data. Although data may be backed up every 10 minutes, it could take an extended period of time to recover the data because of data size.

- Per Object: 5 object (files etc) can be restored at a time (1 object in case of a Tier 2 data centre restore)
- Per Size: 200GB can be restored per hour

Max Priority represents the response time from a resource prospective. If the request to restore occurs during the business hour, the business must contact the Service Desk and state the priority.

RLO (Recovery Level Objective) - This objective defines the granularity with which data can recovered. Examples of RLO: the entire server system, the whole SQL instance, database or set of databases, or specific tables, a single file, an entire Virtual Machine, an entire data volume, a mailbox, an Exchange information store, metadata, configuration

High Availability (HA) – A configuration designed to minimize or mitigate the impact of downtime.

Disaster Recovery (DR) - Disaster recovery efforts address what is done to re-establish availability after an outage. Disaster recovery refers to restoring your systems and data to a previous acceptable state in the event of partial or complete failure of computers due to natural or technical causes.

Record - A record is defined under the Freedom of Information Act 2014 as "any memorandum, book, plan, map, drawing, diagram, pictorial or graphic work or other document, any photograph, film or recording (whether of sound or images or both), any form in which data (within the meaning of the Data Protection Act, 1988 and 2003) are held, any other form (including machine-readable form) or device in which information is held or stored manually, mechanically or electronically and anything that is a part or a copy, in any form of any of the foregoing or is a combination of two or more of the foregoing" (Freedom of Information Act, 2014).

RTO (Recovery Time Objective) - The duration of acceptable application downtime, whether from unplanned outage or from scheduled maintenance or upgrades; the primary goal is to restore full service to the point that new transactions can take place.

RPO (Recovery Point Objective) is the maximum time of data loss that the business application can afford to lose:

- Minutes: Data loss in minutes
- Hour(s): Data loss in hour or more
- Day(s) (24 hrs): Data loss can be up to 24 hours
- Week: Data Loss is non-existent because this is for static data.

Discuss Backup and Recovery Service

If a business owner or project manager want to:

- Discuss the contents of this document, log a call on the Service Desk. This call will be assigned Tech Operations (Tech.Operations@hse.ie)