National Policy for Backup and Restore

National Policy ☒ National Procedure ☐ National Protocol ☐ National Guideline ☐
National Clinical Guideline ☐

DOCUMENT GOVERNANCE [1]	
Document Owner (post holder title):	Deputy Chief Technology Officer
Document Owner name:	James Carrol
Document Owner email contact: *(Generic email addresses only for the Repository)*	Tech.Backup@hse.ie
Document Commissioner(s): (Name and post holder title):	Office of the Chief Information Officer
Document Approver(s): (Name and post holder title):	Office of the Chief Information Officer
Lead responsibility for national implementation:	Technology Backup and Restore Team
Lead responsibility for national monitoring and audit:	Technology Backup and Restore Team
Development Group Name:	Technology Backup and Restore Team
Development Group Chairperson:	Nicky Power
Additional headings can be inserted as required	

DOCUMENT MANAGEMENT [2]			
Date effective from:		16/08/2024	
Date set for next review:		15/08/2027	
Your Reference No: *(if applicable)*		Click or tap here to enter text.	
Current version no:	1	**Archived version no:**	0
Note: Original document is Version 0. First revision is Version 1. Second revision is Version 2, and so on.			
Note: HSE National 3PGs should be formally reviewed every 3 years, unless new legislative/regulatory or emerging issues/research/technology/audit etc. dictates sooner.			

VERSION CONTROL UPDATE [3]		
Version No. (most recent version first)	**Date reviewed** (most recent date first)	**Comments** (1 sentence max, if required)
0	1/8/2019	• Technology Backup and Restore Policy
1	16/8/2024	• Included Cybersecurity Event Recovery • Included Tape Retention of 12 months

[1] Records the senior management roles involved in the governance and development of the document.
[2] Records the control information about the document.
[3] Records details when a document is reviewed, even if no changes are made.

Document management notes:

The National Backup & Recovery Policy has been updated to include a dedicated section on Cybersecurity Event Recovery. The Tape Retention period for Tape backups has been reviewed and updated in line with current best practices and storage efficiency considerations. The new policy reduces the retention period to 12 months.

PUBLICATION INFORMATION [4]
Topic:
Technology Backup and Restore Policy
National Group:
Office of the Chief Information Officer
Short summary:
Establishes a National Standard for backup and recovery.
Description:
This policy establishes 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.

[4] Records the document information required for publication on the HSE National Central Repository.

Purpose

This policy is a comprehensive framework for safeguarding the integrity, availability, and confidentiality of critical data and systems within the HSE. This policy is designed to ensure the efficient and reliable backup of essential information and the recovery of systems in the event of data loss, system failure, or other unforeseen incidents.

Scope

Technology & Deployment manages the Backup and Recovery function.

This policy is only applicable when the Recovery Point Objective (RPO) is equal or greater than 24 hours.

Recovery Point Objective (RPO) is the maximum tolerable period in which the data can be lost. If there is a requirement for a more demanding RPO, the business must implement a High Availability\Failover solution.

The policy outlines the process in recovering an application group or server, this type of recovery will be achieved by a multi-disciplinary team.

A comprehensive list of various data types, along with the recommended backup methodology for each type, ensuring tailored and effective data protection strategies.

A clearly defined schedule for regular backups and a retention policy specifying the duration and criteria for retaining backup data will be outlined, aligning with regulatory requirements and best practices.

The Backup and Recovery policy excludes non-critical Systems such as Test environment.

Audience

The audience for this document eHealth & Disruptive Technologies and HSE business Delivery Directors and Managers.

Backup & Recovery definitions

These key terms are essential for gaining a comprehensive understanding of the Backup and Recovery Service.

Application Group – is the group of servers which the applications needs to function. There may be a number servers required by the application for example Application, Citrix or Database Servers. There also may be dependencies from other applications to provide data input for the environment to function correctly or data output to another application.

Backup Data – The unit of data backed up. Examples of a backup object: File, Folder, Database, Virtual Machine, server volume or System State

Cloned - Cloning is a process involving the duplication of backup data, typically copying the data from a disk-based storage medium to a tape-based storage system.

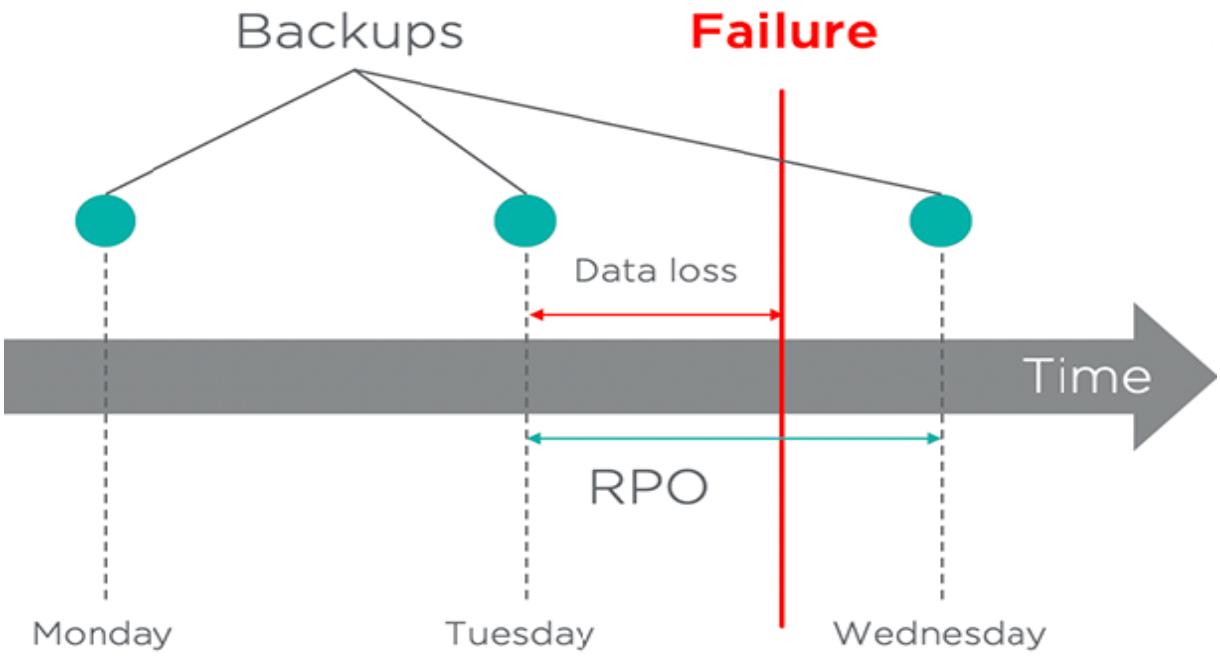
Daily Backup: - is the backup job which run every 24 hours; Backup jobs operate outside of business hours.

Monthly Full Backup: - is the backup job which runs once a month; Backup jobs normally operate over the weekend and outside of business hours.

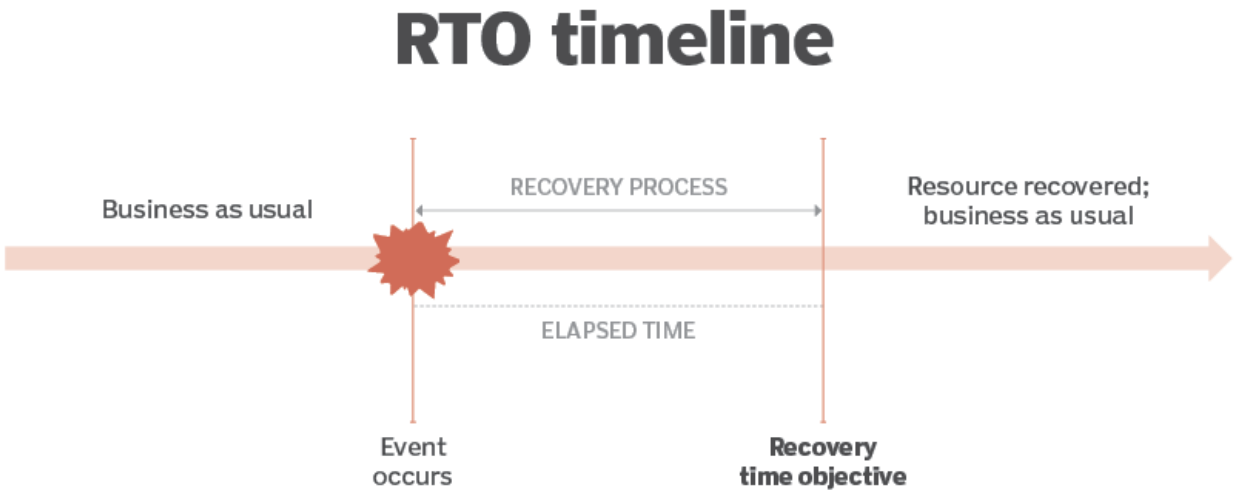
Restore - is the process of recovering file(s), folder(s) or Server(s) from backup data.

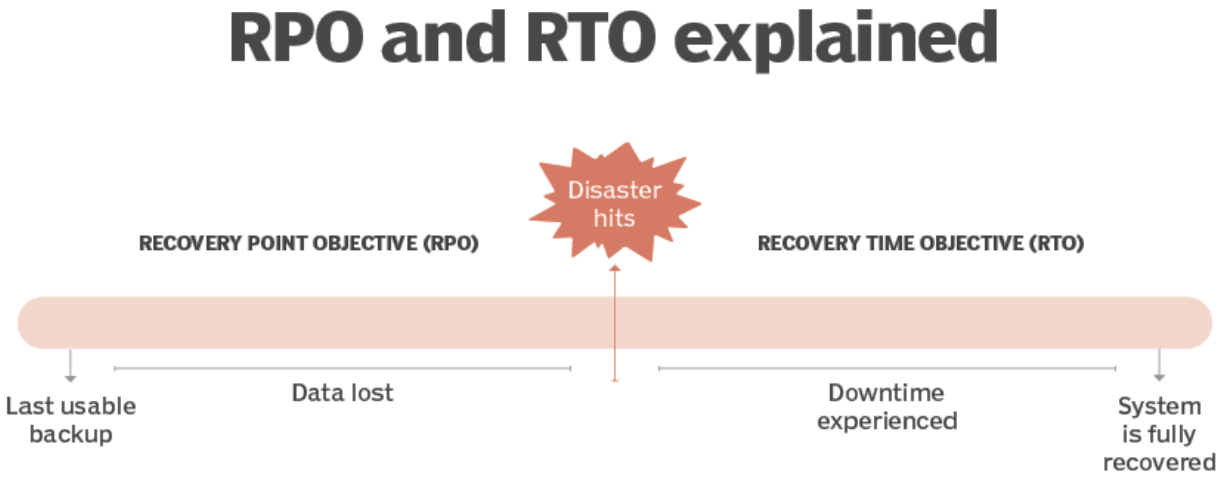
Retention – The length of time the backup data must be maintained and available for a restore.

RPO (Recovery Point Objective) determines loss tolerance and how much data can be lost. It is a planning objective that defines how often data needs to be backed up to enable recovery.



RTO (Recovery Time Objective) - is the maximum tolerable length of time that a computer, system, network or application can be down after a failure or disaster occurs.





Datatypes and their backup methodology

This policy discusses the backup methodology for each datatype outlined below. The datatype(s) must be identified during the service adoption process described elsewhere in the document.

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. This also includes opened files.

Office 365 (O365 & Dynamic 365):

The backup policy for Office 365 (including O365 and Dynamics 365) must adhere to the following guidelines:

Exchange Online:

All emails, calendars, contacts, and other mailbox items within Exchange Online are backed up using Cloud Backup Solution compatible with Office 365.

SharePoint Online:

Data stored in SharePoint Online, including documents, lists, libraries, and site collections, must be backed up using Cloud Backup Solution compatible with Office 365.

OneDrive for Business:

User files and data stored in OneDrive for Business accounts are backed up using Cloud Backup Solution compatible with Office 365.

Microsoft Teams:

Microsoft Teams are backed up using Cloud Backup Solution compatible with Office 365.

Dynamics 365:

Data within Dynamics 365 applications will be backed up using Cloud Backup Solution compatible with Dynamics 365

Email\Exchange Online:

All emails that reside in the sent to and from email box 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: the Backup and Recovery service provides backup via agent or snapshot for the following operating systems: Windows 2012 Server and above, and Linux supported kernel.
Citrix Servers: the Backup and Recovery service provides backups of these servers via snapshots.
Database Servers: the Backup and Recovery Service provides backup of the server via an Snapshot.

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 is backed up via a Database maintenance job; this method must be deployed and it is the responsibility of the Database Administrator.

Oracle: Database is backed up via the RMAN (Recovery Manager) tool which can keep the database online during backup operations. The Database Administrator is responsible for this method.

MYSQL: Database is backed up via a script or tool which must be managed by the Database Administrator. The Database Administrator is responsible for this method. The backup files are stored to a share which is backed up by the backup software.

Active Directory:

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

.

Out of scope

The Backup and Recovery Service does not support all data types. Specifically, the following data is not covered, regardless of its type:

- Physical Data, stored on paper, USB devices, CDs etc (NAS)
- Data that is not stored in an HSE Tier 1 (National) or Tier 2 (Regional) data centre or Cloud Tenant
- Data that is stored on a client, mobile or other non-supported devices
- Data in Transit (Is the responsibility of the Transport Layer)
- Data in memory / cache / swap files
- Development, Test, Training & Staging Servers are not backed up. These are identified by the first letter in their hostname (R = Training, S = Staging, T = test & D = development)
- **Unmanaged device** which is a device that has not been procured through the Technology. These devices are typically set up, configured, and maintained by individual users or departments outside of the centralized Technology infrastructure.

Backup Schedules & Retention

The following backup schedules outlined below:

- Daily incremental:
  - Normally Operates between non Business hours 5pm and 9am.
  - Backup data is coped to a specific backup target.
  - Retention of 3 months (90 Days) on the backup targets.

- Monthly Full:
  - Operates on a Friday of every Month
  - Backup data is coped to a specific backup target. This data is cloned to tape.
  - Retention of Backup Data on the backup targets.
    - Disk: - 3 Months (90 Days)
    - Tape: - 12 Months
- Backup Targets:
  - Data will be no longer be available after the retention period expired:
    - Disk: 3 months (90 Days)
    - Tape: - 12 Months
    - Cloud: - 12 Months

- Exceptions:
  - Database Servers follow the Monthly Full schedule only; the database backups are managed by the DBA Services Maintenance jobs where the databases are backed up to a separate location, as described at the Databases datatype.
  - Citrix Servers follow the Monthly Full schedule only.
  - Emails passing through any on premise HEALHTIRL managed email server and deleted on same day will not be included in the daily and monthly schedules.

All other individual exceptions must be agreed upon and documented during the Service Adoption phase. However, these exceptions must fit within the existing schedules mentioned above. Creating new schedules or changing the existing standard schedules for individual needs is not supported.

Schedule for server types are outlined below. The backup schedule is determined by Server Type.

Backup Schedule				
Server Types	**Daily (Incremental)**	**Weekly (Full)**	**Monthly Full**	**Example**
File Server	Yes	Yes	Yes	File Shares: - Files are modified on a daily basis then daily backups must be performed
Mail (on premise Exchange)	Yes		Yes	Exchange (016, 019), change on a regular basis then daily backups must be performed
Application Server	Yes		Yes	Business applications, Citrix, Proxy, DNS, DCHP, Web Servers: - these servers store files which are updated frequently then daily backups must be performed
Database – Microsoft SQL			Yes	The database administrator must complete a backup of the database (daily) and transaction logs (every x minutes) via a maintenance job written to a secondary target. This share must be backed up and written to tape daily. The Server backup does not include the database during this backup job.
Database – ORACLE	Yes		Yes	The database administrator must back up the database using the RMAN (Recovery Manager) tool. The DBA can request a share to be created to allow the database backup to be created on a secondary target. Daily backups must be performed
Database – MYSQL			Yes	The database administrator must back up the database using a script or tool. The DBA can request a share to be created to allow the database backup to be created on a secondary target. Daily backups must be performed
Database – Another (Other databases not defined above)			Yes	The database administrator must back up the database using a script or tool. The DBA can request a share to be created to allow the database backup to be created on a secondary target. Daily backups must be performed
Active Directory	Yes		Yes	Active Directory: - Daily backups must be performed.

Cybersecurity Event Recovery

With the volume of significant cyber incidents on a rise annually which exploits company's vulnerabilities in systems, individuals, and technologies. It is widely acknowledged that some of these cyber events are inevitable, so exclusively prioritizing prevention is not effective. The HSE have enhance their preventive measures using cutting-edge technology and tools, to detect and respond to cyber incidents.

NIST SP 1800-11, Data Integrity: Recovering from Ransomware and Other Destructive Events

There is three backup copies available to a recovery process depending on the nature and extent of the attack as defined within the Respond phase. Recovery should always be the closest feasible data copy to live data as possible to minimise the recovery process. Backup Data is stored on the Cyber vault infrastructure.

NIST SP 1800-25, Identifying and Protecting Assets against Ransomware and Other Destructive Events

Identifying: All Production servers and data must be included for backup and protection operation

Protect: These three data Backup copies are stored different levels of significance in terms of their resilience. Zero trust factors (PR-AA-01-05) and data immutability for example would be applied to the first 2 copies in site redundant locations. The third copy is extracted into a secure off-network, air-gapped vault which is kept away from the attack surface of a ransomware attack (PR-IR-01).

NIST SP 1800-26, Detecting and Responding to Ransomware and Other Destructive Events

Detect: In addition to detection techniques in the live environment, very specific data integrity checking is performed on a daily basis for assets backed up. This analysis job would uniquely interrogate the full contents of the backed-up data within a controlled and secure manner in the vault and report on suspicious data detected (PR-PS-04) using over 200 sets of heuristics and data patterns that are programmed into the analysis algorithm (DE.CM-02 specific to backup data).

This detection process then informs the HSE team which data is affected, what user it belonged to and significantly, which data is clean to allow a recovery to take place (DE.AE-02-07 specific to backup data).

Respond: The data detection techniques available in the vault are not processing data in real time, but depending on the nature of an attack and whether compromised data was extracted into the vault over time (e.g. silent encryption); some intelligence to assist with forensics processes may be available from the vaulted backup data.

Tape Management

Tape backups are not completely 100% reliable for data recovery.

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 secure area.
- Removable media must be stored in a temperature and humidity controlled environment. Do not store on radiators, window sills, electronic equipment or machinery. Keep out of strong sunlight and avoid contact with water.

Storage of Backups

Tapes must be stored onsite (in a locked, accessed controlled area), offsite at an Irish Government Storage Facility or in a Third Party Storage facility.

- In all locations:
  - Media should be clearly labelled with unique bar codes that tie into the backup management package.
  - The media in the facility must be audited annually; to ensure all the media that was transmitted is present.

- 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

Encryption

Backup Tapes must not be encrypted.

By encrypting tapes would 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.

Service Reporting

To ensure a minimum of 95% backup success rate for all critical data. This will be achieved through rigorous monitoring, regular maintenance, and continuous improvement of the backup infrastructure.

The following reports are available to Tech Backup Team:

- Any Backups jobs modified
  - Audit trails
- Backup Success Rate (Daily, Weekly, Monthly and Yearly)
  - Drill down to specific servers
    - Infrastructure Daily Backups
    - Business Weekly Backups (available internally)
- Backup Failure Rate (Daily, Weekly, Monthly and Yearly)
- Backup Disk Capacity
  - Timelines available
- Recovery Readiness
- Backup Data growth

Service Description

The purpose of this service is to ensure the organization's data is protected in the event of:

- Data Corruption
- Equipment failure
- Intentional destruction of data

For this purpose, the services provided:

- File based Backup & Recovery
- Application Group Recovery
- Backup Media management

Technology & Deployment Teams manages the function the Backup and Recovery Service. The Business Delivery Director's Team is responsible for ensuring that their Application & systems are backed up and recoverable.

Backup and Recovery administrators must follow the following guidelines:

- Access\Confidentially: Backup Administrators can only access the backup data. The restored data must only be stored in a location, which is accessed, by the requestor and backup administrator.
- Reliability (Available & Integrity): Backup Administrators must restore the actual data which was backed up at the specified time. The administrator must perform the restore within the agreed service level.
- Disposal: Backup Data must be stored on Disk or Tape for the agreed retention time. The data on those tapes must be destroyed after they have reached their retention time. Restore data must be stored in a temporary location for the requestor before it must be deleted. Backup devices can be recycled in accordance with the requirements of the European Waste Electrical and Electronic Equipment (WEEE) Directive. Users must notify the eHealth of any old I.T. devices and equipment and they must facilitate the collection and disposal of the devices and equipment as per HSE IT Acceptable Use Policy.

Data Centre

There are 3 tiers defined for Data centres:

- Tier 1: - National data centre: the targets used for all backups is Disk. The Monthly Full backup is cloned from Disk onto Tape on a monthly basis. Tapes are stored off site in an Iron Mountain facility.
- Tier 2: - Regional data centre: the targets used for all backups is Disk. The Monthly Full is cloned from Disk onto Tape on a monthly basis. Tapes must be removed from Tape Library by local EHealth staff and stored in a fire-proof safe. The safe must be located in a secure location and prohibited from unauthorised access.
- Tier 3: - Non-standard room where server(s) are in operation. This is not a data centre: The policy does not cover this type of Data Centre.

The scope of the Technology & Deployment Teams is only limited to Tier 1 and Tier 2 data centres. **Tier 3 data centres are explicitly out of scope for this document.**

Backup software:

- Tier 1 & Tier 2: - An enterprise software solution must be deployed at these Data Centres.
- Tier 3: - Out of scope.

Service Requests

File(s) or Folder(s) Restore request

Any Restore required during business hours must be submitted to the National Service Desk. The Service Desk can be contacted on **0818 300 300** from 9:00 to 17:00 hrs Monday to Friday. The requestor must provide the restore details such as server name, the full location of the file and date of the file to be restored. The requestor must receive an automated email with a summary and ticket reference.

If there is a requirement to restore after business hours specified above, the requestor must contact the Out of Hours Support.

Application Group or Systems Recovery Request

If there is a requirement to recover an Application Group or individual server, the Critical Incident Team must be notified.

The Critical Incident Team will bring all the relevant teams together to decide on the recovery route.

Teams:

- Application Support
- Business Delivery Director \ Team
- Critical Incident Team \ IT Recovery Manager
- DBA Services
- Technology & Deployment
- Vendors

Appendix

A. Document References

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

HSE Information classification policy:
hsenet.hse.ie/EHealth/Service_Management/PoliciesProcedures/Policies/HSE_Information_Classification_Handling_Policy.pdf

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

B. 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.

The Information Classification Policy (see the appendix for a link to the policy document) outlines the following classes of information:

Public Information
Public information is defined as information that is available to the general public and is intended for distribution outside the HSE. There would be no impact on the HSE, its staff, clients or patients if this type of information was mishandled or accidentally released. Some examples of public information include:

- Patient/Client brochures
- Staff Brochures
- News or media releases
- Pamphlets
- Advertisements
- Web content
- Job postings
- Public Health Information

Internal Information
Internal information is defined as information that is only intended for internal distribution among HSE staff, students, contractors, sub-contractors, agency staff and authorized third parties (i.e. service providers etc). In the majority of instances there would be no significant impact on the HSE, its staff, clients or patients if this type of information was mishandled or accidentally released. Some examples of internal information include:

- Internal telephone directory;
- Internal policies & procedures (excluding those published on the web);
- User manuals;
- Training manuals and documentation;
- Staff newsletters & magazines;
- Inter-office memorandums (depending on the content);

- Business continuity plans.

Confidential Information
Confidential information is defined as information which is protected by Irish and/or E.U. legislation or regulations, HSE policies or legal contracts. The unauthorised or accidental disclosure of this information could adversely impact the HSE, its patients, its staff and its business partners.
Some examples of confidential information include:

- Patient / client / staff personal information (Except that which is restricted)
- Patient /client / staff medical records (Except that which is restricted)
- Unpublished medical research
- Staff personal records
- Financial information / budgetary reports
- Service plans / service performance monitoring reports
- Draft reports
- Audit reports
- Purchasing information
- Vendor contracts / commercially sensitive information
- Information covered by non-disclosure / confidentiality agreements
- Passwords / cryptographic private keys
- Information collected as part of criminal / HR investigations
- Incident reports

Restricted Information
Restricted information is defined as highly sensitive confidential information. The unauthorised or accidental disclosure of this information would seriously and adversely impact the HSE, its patients, its staff and its business partners. Some examples of restricted information include:

- Patient / client / staff sensitive personal information;
- Childcare / adoption information;
- Social work information;
- Addiction services information;
- Disability services information;
- Unpublished financial reports;
- Strategic corporate plans;
- Sensitive medical research.

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 **Restricted Information**.

C. Guide for **Cybersecurity** Event Recovery

This document is not an operational playbook; it provides guidance to help organizations plan and prepare recovery from a cyber-event and integrate the processes and procedures into their enterprise risk management plans.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf