

## **Information Management Policy**

### **1. Introduction**

1.1 This policy sets out the way in which all information is managed by HITRANS, as required to achieve sound and effective corporate governance.

### **2. Scope**

2.1 This policy applies to HITRANS employees, Board members, advisors and all other individuals and third parties who have access to HITRANS information and systems.

2.2 This policy applies to all the information HITRANS holds, regardless of its format or whether it was created within or outwith HITRANS.

### **3. Information Principles**

3.1 The information management principles define the supporting policy statements. The Information Principles are:

- HITRANS information is a corporate asset.
- We are personally responsible for the management of the information we create, capture, store and use.
- We will manage information to ensure compliance with statutory and regulatory requirements and good practice.
- We will make information available appropriately throughout the lifecycle of the resource, including records identified for permanent preservation.
- We will manage information throughout its lifecycle.
- We will ensure that information is accurate and fit for purpose.
- We will retain or dispose of information appropriately following Data Protection Policy and Information Management Policy.
- We will make information freely available when required following Freedom of Information Policy.

### **4. HITRANS information is a corporate asset**

4.1 We acknowledge that information is frequently created or received by individuals within HITRANS, and that the contribution of individuals is essential to achieving our business objectives, however, information as a resource is "owned" by HITRANS.

4.2 Information, digital and physical, and the systems used to create, access, use, store, manage and dispose of information will be treated as valuable corporate assets.

## **5. We are personally responsible for the management of the information we create, capture and use**

5.1 The responsibility for how information is managed and used on a day-to-day basis lies with individuals within HITRANS.

- Individuals are responsible for ensuring that the information they create or acquire is properly managed following Corporate guidance detailed in the Information Management Policy and also where published on the intranet.
- Everyone within HITRANS is responsible for the security of information and ensuring that sensitive information does not get into the wrong hands.
- All HITRANS staff who engage others to represent or work with HITRANS e.g. system suppliers, sub-contractors, consultants etc. are responsible for putting in place required controls and obligations in line with Standing Orders and supporting documents.

5.2 Senior Management will ensure that there will be regular briefings on Information Management and Security communicated to employees to ensure each knows their responsibilities for information management and security, including their responsibilities in managing contractors and relevant third parties.

## **6. We will manage information to ensure compliance with statutory and regulatory requirements and good practice**

6.1 Information security controls will be applied to protect personal and other sensitive information in accordance with relevant legislation.

- The Staff Induction Programme and Code of Conduct for Members and Officers support this policy.
- We will make assessments of HITRANS computer systems against recognised standards for Information Security management, including ISO/IEC 27001:2005, and where appropriate ensure compliance.

6.2 The controls needed to ensure the protection and security of HITRANS's assets will be determined by a process of Risk Assessment and Analysis.

- This will determine the existing vulnerabilities of assets, the threats to them, and the potential impact on HITRANS if there were a breach of security.

## **7. We will make information available appropriately throughout the lifecycle of the resource, including records identified for permanent preservation**

7.1 Staff are responsible for access to information they create or hold.

- Staff will manage information they create or hold in accordance with the Information Security Classification.
- Information sharing will support better decisions, and the ability to reuse information improves efficiency and effectiveness. Staff will make information they create or hold accessible to as wide an audience as is possible while fully respecting legislative and regulatory obligations, especially for personal and other sensitive information.
- Data sharing with third party organisations requires specific data sharing protocols and data processing agreements.

7.2 The goal is to create, store and manage information once for use many times, where the technology allows. Storing multiple copies of information reduces the ability to manage appropriately, and reduces identification of the correct version.

## **8. We will manage information throughout its lifecycle**

8.1 Information will be stored in Corporate repositories, where it will be managed in accordance with this policy and supporting policies and procedures.

8.2 HITRANS will implement an Information Security Classification to assist in the identification of behaviour required to manage our information resources.

8.3 Information will be labelled following Corporate guidelines to allow searching and finding of relevant information, and to understand the value of the information and its availability for use.

8.4 Links to information rather than attachments will be used in emails, where at all possible, to reduce the multiplication of instances of the information resources. This will enable the preservation of “one version of the truth” and reduce storage space and the costs associated with it.

## **9. We will ensure that information is accurate and fit for purpose**

9.1 Information will be accurate and fit for purpose and the publishing process will be supported by a review and approval process to ensure consistent quality and appropriate content. Review dates will be applied for published electronic information.

9.2 Information will be presented in compliance with obligations to specific audiences, and will consider the Disability Discrimination Act.

## **10. We will retain or dispose of information appropriately following appropriate guidance and Data Protection Policy**

10.1 This Policy is in support of the Data Protection Policy and appropriate guidance within the Standing Orders where indicated that information will be created, collected and stored as appropriate to the business need, and is retained only for as long as it is needed to carry out its statutory functions, service provision and community obligations whilst having due regard to legislative and evidential requirements.

## **11. We will make information freely available when required following Freedom of Information Policy.**

11.1 This policy is in support of Freedom of Information Policy, and recognises the benefits of making information available to the public, and how this helps build public trust and confidence in the work of HITRANS.

## **12. Key Provisions**

### **12.1 Policy Owner**

- This Information Management Policy is owned by the Partnership Director, who is ultimately responsible for Information and Security within HITRANS. This Policy will be reviewed at least annually.

## Responsibilities

Commitment	Responsible
Approval of Information Management Policy	Partnership Director
Internal Communications	Office Manager
<p>Develop and Publish all supporting information related to policy, procedures and guidelines</p> <p>Review and approve all supporting information related to policy, procedures and guidelines</p> <p>Review compliance with information policy, procedures and guidelines</p> <p>Approve deviations from information management policy procedures and guidelines</p>	Partnership Director
<p>Develop and publish supporting records management related policy, procedures and guidelines</p> <p>Review and approve all supporting records management related policy, procedures and guidelines</p> <p>Review compliance with records management related policy, procedures and guidelines</p> <p>Approve deviations from records management related policy, procedures and guidelines</p>	Partnership Director
Review compliance with appropriate Data Protection and Freedom of Information legislation	Web developer and Partnership Managers All Contractors and third parties

<p>Develop and publish information security related policy, procedures and guidelines</p> <p>Review and approve all information security related policy, procedures and guidelines</p> <p>Review compliance with information security related policy, procedures and guidelines</p> <p>Approve deviations from information security related policy, procedures and guidelines</p>	<p>Partnership Director</p>
<p>To instruct and manage employees as they undertake personal processes:</p> <ul style="list-style-type: none"> <li>• Induction process</li> <li>• Personal Development Plan to provide support and training to support information management</li> <li>• Exit process including interview</li> </ul>	<p>Partnership Director</p>
<p>Employees to participate and feed into personnel processes:</p> <ul style="list-style-type: none"> <li>• Induction process</li> <li>• Personal Development Plan to provide support and training to support information management</li> <li>• Exit process including interview</li> </ul>	<p>All Staff</p>
<p>Ensure staff manage information appropriately through its lifecycle by following policy, procedures and guidelines.</p> <p>Ensure staff have access to the appropriate technology to allow them to securely manage information, e.g. encryption of laptops and other portable devices and secure storage</p>	<p>Partnership Director</p>

<p>Support the User Access Management Process i.e. inform System Owners (Information Asset Owners) of staff and role changes</p>	
<p>Manage information appropriately throughout its lifecycle by following legislative and good practice guidance and the associated policy, procedures and guidelines.</p> <p>To use secure technology where provided and highlight to managers instances where there are gaps in the technology.</p>	<p>All Staff</p>
<p>Appropriate information management considerations applied to information systems</p>	<p>All Staff</p>
<p>Inclusion of information management guidance in training materials and courses</p>	<p>Employee development</p>
<p>Information and Records Management roles and responsibilities to support Service delivery.</p> <p>Assurance and coordination of Information Management practices. Administration of corporate information management systems</p> <p>Assurance and coordination of Records Management practices</p> <p>Administration of corporate Records Management processes.</p>	<p>Office Manager</p>

## Document Version Control

<b>Records Management Plan</b>	<b>Group or Name(s) &amp; Designation(s)</b>	<b>Date</b>	<b>Version</b>
Author:	Ranald Robertson	27/01/2013	v.1.0
Owner:	Ranald Robertson	27/01/2013	
Approved by:	HITRANS Partnership Board	08/02/2013	
Reviewed/Updated	Ranald Robertson	23/11/2016	v.2.0

**Changes to the document (e.g. as part of annual review or following a change to elements) should be approved by the HITRANS Director.**