ICRIR

Independent Commission for Reconciliation and Information Recovery

Annual policy statement regarding Section 34 regulations - holding and handling of information.

12 December 2024

Introduction

1. Regulation 2 (1) of the Independent Commission for Reconciliation and Information Recovery (Holding and Handling of Information) Regulations 2024 requires the Independent Commission for Reconciliation and Information Recovery ("the Commission") to put in place a policy document in relation to the holding and handling of information by the Commission.

2. Regulation 2 (2) states that the document must explain the Commission's policies and procedures for:

    a. securely accessing information held by others (including information which is to be transferred to the ICRIR);
    b. the secure receipt of information being transferred to the ICRIR;
    c. the secure retention of information by the ICRIR;
    d. the secure destruction or transfer of information which is to cease to be held by the ICRIR;
    e. managing and investigating any breaches of the ICRIR's policies and procedures in relation to the holding and handling of information (which must include the reporting of all breaches to the Chief Commissioner).

3. In addition, regulation 3 states that no later than six months after the end of each financial year, the Commission must appoint a person or persons to review the Commission's policies and procedures in relation to the holding and handling of information by the Commission.

4. The document must be published when the Commission first publishes an annual report. The first annual report is published on 12 December 2024.

5. This document sets out the required details for the regulations and is the first issuance of such a policy document.

Commission roles and responsibilities

6. All Commission staff are responsible for ensuring information, and any associated risks are managed appropriately. To ensure that responsibility for delivering strong standards of information management practice is embedded throughout the Commission, we have an induction and ongoing training programme delivered across all employees. This covers information security, policies and expectations of staff.

7. The Commission also assigns specific roles to individual staff members relating to information security. These staff are provided with specific guidance covering their roles and responsibilities. The main roles are:

    a. Data Protection Officer (DPO)
    b. Senior Information Risk Owner (SIRO) - the Chief Operating Officer
    c. Information Asset Owners (IAOs)
    d. Information Asset Managers (IAMs)

e. SharePoint Site Owners (SOs)
f. Security Adviser (SA)

8. The Audit and Risk Committee (ARC) is a senior level board committee and sits at the heart of the Commission to ensure that Commission information is appropriately managed and kept secure. It is chaired by the lead Non-Executive Commissioner and consists of at least two non-executives plus an external independent member.

9. The ARC provides overview and scrutiny of information governance arrangements. Information risks are escalated to the SIRO for decisions. The Information Security team are tasked with developing the information risk appetite statements and maintaining a risk register.

10. Central support to this network is provided by several teams within the Commission with responsibilities and appropriate skills to deliver the following functions:

    a. Information Management
    b. Information Security
    c. Risk Management
    d. Information Access
    e. Facilities
    f. IT
    g. Legal
    h. Procurement
    i. Human Resources

The Legislative Framework

11. The Commission adheres to all relevant statutory frameworks, regulations, guidance and codes of practice to meet our information management responsibilities. This includes:

    a. UK General Data Protection Regulation (UK GDPR)
    b. Data Protection Act 2018 (DPA 2018)
    c. Freedom of Information Act 2000 (FOIA 2000)
    d. The Government Functional Standard GovS 007: Security – Version 2.0 13 September 2021
    e. The HMG Personnel Security Controls – Version 6 2022
    f. The Government Security Classifications Policy – 30 June 2023
    g. International Classified Exchanges – Version 1.5 March 2020
    h. Guidance: Protecting international RESTRICTED classified information – Version 1.3 March 2020
    i. The Information Commissioner's Code of Practice.

Security classifications

12. Information the Commission receives, stores, processes, generates or

exchanges as part of the investigative process or organisation's administrative corporate functions should be handled in a manner that is appropriate to its sensitivity.

13. Classifying information is a crucial step in managing information as it indicates the sensitivity of information and the typical controls necessary so the appropriate level of protection can be put in place. The Commission will ensure that its material is properly classified in accordance with the Government's Security Classifications Policy and where relevant, the Government's Guidance on International Classified Exchanges.

International partners classified information

14. We will consider compliance in all relevant countries where the Commission transfers information across jurisdictional borders where laws and regulations can affect the Commission.

15. When accessing, retrieving, storing, transferring and disposing of information held by international partners, the Commission will comply with the principles and procedures set out in the Government's Guidance on International Classified Exchanges and the Government's Guidance on Protecting International Restricted Classified Information.

Vetting and security clearance

16. The security of Commission data and information sits within the overall Commission approach to security and risk including Information and Communications Technology (ICT), security vetting of staff (personnel security) and the physical security of our estate.

17. In line with the HMG Personnel Security Controls Policy referred to in the regulations, the Commission undertakes National Security Vetting (NSV) on employees who require access to specific information, sites or systems. NSV is delivered by the United Kingdom Security Vetting (UKSV), via a commercial arrangement with the Commission, and ensures that the Commission identifies, manages and mitigates any risks where national security is a focus. Any information obtained and stored by the Commission will always be handled by staff with the appropriate security clearance.

Securely accessing and receiving information held by others

18. The Commission has a range of statutory powers available to access and retrieve information held by others. Further information on how the Commission recovers information can be found in the Commission document 'How the Commission Shares and Publishes Information'. The Commission will ensure that material is only viewed, accessed and handled by people with the relevant security clearance and in locations and in a manner that is consistent with the Government's Security Classification's Policy.

Secure storage of information

19. Whether it is electronic or hard copy, we store our information in prescribed locations, appropriate to its format, content, and sensitivity. We ensure appropriate controls are in place to maintain the confidentiality, integrity, and availability of our information. We have technical and organisational measures in place to ensure information is protected, including: encryption of our data and IT equipment; physical security measures; regular data protection training for our staff; regular testing of our technology; and restricted access controls (i.e. measures to ensure only people who need to access your Personal Data are able to do so). The Commission Privacy Notice sets out how we use your personal data and your rights.

20. In relation to hard copy material, the Commission operates a clear desk policy. Moreover, the Commission estate is designed to ensure it is as secure as possible from a physical perspective. This includes pass protected entry into certain areas of the estate, installation of CCTV and extra levels of security to protect the most sensitive information held.

Securely managing the retention and disposal of information by the Commission

21. Our Data Retention and Destruction Policy outlines our approach to managing the retention and secure disposal of our information. It provides for a consistent approach and applies to all physical and digital information, regardless of storage location.

22. Our retention periods are driven by legislation or business need. The Data Retention and Destruction Policy governs most information retention, and if there is no legally defined retention period for corporate information, it is the responsibility of the relevant IAO (with input from the Data Protection Officer) to determine an appropriate retention period.

Managing and investigating any breaches of the Commission's policies and procedures in relation to the holding and handling of information

23. Ongoing monitoring of compliance with this policy and its supporting policies, guidance and procedures will be undertaken on a regular basis by the Security Advisor and supported by those in the Information Risk Management Network, with external checks as appropriate.

24. The Commission has its own internal Assurance Team which is responsible for monitoring adherence to all operational policies across the Commission. The Commission has appointed an external security specialist to assess, review and assure all relevant information security policies, systems and processes in-line with the requirements of the Government Cyber Security Standards. This assurance process will be undertaken on a regular basis, at least annually as per the requirements of the regulations.

25. The Commission recognises the importance of holding and handling data in a responsible and lawful manner. All security incidents, or potential incidents, are taken seriously and investigated in a swift and proportionate manner.

26. In accordance with the Government's Security Classifications Policy, all staff should be aware that they are required to detect, report and respond to all security incidents. They must report a potential breach as soon as it comes to their attention so that it can be reviewed, appropriately actioned and referred, if necessary, to the police or the Information Commissioner's Office within the statutory 72-hour deadline. All incidents will be brought to the attention of the Executive Leadership Team (ELT) and regular reporting on security incidents will be provided to both the ARC and the Board of Commissioners.

Document update and review

27. Within six months of the annual report's publication, the Commission will appoint an independent person(s) to review the Commission's information handling and holding policies and procedures and the external assurance provider will produce a report for the Commission. The Commission will assess any recommendations within the report and make any required changes to the information security infrastructure, policies and processes. As per the requirements of the regulations, any changes will be reported on at the publication of the next annual report.

28. The Commission ELT is responsible for this document. The related assurance process is the responsibility of the Commission's Chief Operating Officer.