ESDC Storage of Electronic Information Directive

1. Effective Date and Annual Review

This Directive took effect on its approval by the ESDC Corporate Management Committee (CMC) on February 4, 2015, and was modified on November 25, 2019. It will be reviewed annually by the Innovation, Information and Technology Branch (IITB).

2. Audience

This Directive applies to all individuals (including employees, casuals, and contractors) who have been granted access to the Employment and Social Development Canada (ESDC) electronic network.

ESDC includes Service Canada and the Labour Program, and is collectively referred to as “the Department” or “departmental".

3. Purpose

3.1 This Directive identifies the unstructured repositories available for storing work-related information within or connected to the departmental electronic network, and defines the information content permitted in each one.

3.2 This Directive should be read in conjunction with the ESDC Portable Storage Devices Directive, as well as other policies and directives related to IT security and information management (see References).

3.3 This Directive responds to Treasury Board (TB) direction that proper storage is essential for both the safeguarding and authorized retrieval of departmental information.

3.4 This Directive supports the use of emerging technological solutions where information will be managed, such as cloud computing, and an Electronic Document and Records Management System (EDRMS).

4. Basic Requirement

All departmental unstructured electronic information must be properly stored on the ESDC electronic network, in accordance with this Directive.

5. Detailed Requirements

5.1 Responsibility

Individuals are responsible for the proper handling, storing and safeguarding of information, including electronic information. This includes determining the classification of information as outlined in the Information Classification Guide, or by consulting a manager or the office of the Departmental Security Officer (DSO).

5.2 Table of Permitted Electronic Information Storage Options

There are several types of information repositories used in the Department, depending on requirements and evolving technologies; security capacities vary in each type. The following table shows current repositories and the permitted information content for each.

REPOSITORY	PERMITTED	NOT PERMITTED
NOTE: Personal information that is not related to an individual's work or employment is not permitted on any departmental media or network drive.		
Local Fixed Storage (e.g. C: drive, Desktop)		Information must not be placed on local fixed storage unless required by job function.
Personal Work-related Network Storage (F: drive)	Work-related personal information (examples include personal administrative forms).	Work-related information (both information resources of business value [IRBV], and transitory information). These must be stored in a common repository. Personal information that is not work-related. The total size of individual F drives must not exceed 2 GB.
Collaborative Repositories (e.g. U: drive, SharePoint, Knowledge Portal, Intranet collaboration sites)	Work-related information up to and including Protected B; and temporarily, work-related personal information. (*Temporary* display of team social activities such as retirements, team-building activities, awards ceremonies))	Work-related information above Protected B.
Sensitive Document Collaboration Service	Work-related information Protected C, Confidential, or Secret. Note that only individuals with valid security clearance at the Secret level can have access to the Sensitive Document Collaboration Service.	Work-related information Protected B and below.
Approved Encrypted USB Portable Storage Device	Work-related information up to and including Secret.	Work-related information above Secret.
Approved (exception basis) Un-encrypted USB Portable Storage Devices	Unclassified information only.	Work-related information Protected A and above.
CD/DVD (Exception based)	Work-related information up to and including Protected A.	Work-related information above Protected A.
Internet based websites, Social Media, Collaboration sites	Unclassified information only.	Work-related information Protected A and above.
Extranet Government Collaboration sites (GCPedia, GCConnex, GC Forums)	Unclassified work-related information only.	Work-related information Protected A and above.
Departmental Email System	Work-related information up to and including Protected B. See Information Classification Guide	The department's email system should not be used as a storage repository. The email system is for transitory information purposes only. The total size of any email account must not exceed 2 GB. Exceptions may be granted for defined reasons.
Departmental Smartphones (approved to connect to ESDC email)	Transitory work-related information up to and including Protected B, on the "work side" of a smartphone.	Devices must not be used as a storage device. IRBV must be moved to a corporate repository.
Departmental Cellular Phones (not approved to connect to ESDC email)	Transitory work-related to information up to and including Protected A.	Devices must not be used as a storage device. IRBV must be moved to a corporate repository.

6. Definitions

TERM	DEFINITION
Classified information	Contains sensitive information classified Confidential, Secret or Top Secret; see Information Classification Guide.
Data loss prevention	Prevention of potential breaches by monitoring, detecting and blocking sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage).
Information life cycle	The life cycle of information management encompasses the following: planning; the collection, creation, receipt, and capture of information; its organization, use and dissemination; its maintenance, protection and preservation; its disposition; and evaluation.
IRBV	Information resource of business value.
Unclassified information	Information which is neither Protected nor Classified.
Personal information (not work-related)	Information or files unrelated to an individual's work or employment in the Public Service. This includes, but is not limited to, music, photos, videos, and documents of a personal nature.
Personal information (work-related)	Information or files related to an individual's work or employment, such as resumes, job postings, job applications, letters of offer, competition materials, training, study materials, performance agreements, grievances, as well as reference materials and personal task management documents.
Protected information	Contains sensitive personal, private, or business information classified Protected A, B or C; see the Information Classification Guide.
Repository	A storage location for information, using any of a variety of technologies.
Sensitive Document Collaboration Service	Restricted File Service is used to reduce risk and increase collaboration functionality for the processing of materials classified Protected C or Confidential, or Secret.
Transitory information	Information that is only required for a limited period of time and has no business value.
Smartphone	A mobile phone that is approved to connect to work email (BlackBerry, iPhone, Samsung)
Cellular Phone	A mobile phone that **is not** approved to connect to work email.

7. Monitoring and Reporting

Security measures are actively applied to all IT domains in order to provide efficient, effective, and secure management of all work-related information stored on the departmental electronic network, associated systems, and information storage devices.

IITB monitors and reports on information storage practices across the electronic network to support the requirement of compliance with this Directive.

8. Consequences

Individuals will be held accountable for complying with this Directive. Failure to comply with this Directive may result in administrative and/or disciplinary measures being taken, up to and including termination of employment.

9. Enquiries

Questions regarding appropriate information storage or the application of this Directive should be directed to NA-ITSCOE-CEMSTI-GD@servicecanada.gc.ca

10. References

ESDC

- ITSCOE Policies, Standards, Guidelines and Report
- ESDC Information Classification Guide
- ESDC Code of Conduct
- The most recent versions of the following IM/IT policies can be found in iService References:
  - ESDC Cellular Services Directive
  - ESDC Network Use Directive
  - ESDC Personal Computing Devices Directive
  - ESDC Portable Storage Devices Directive
  - ESDC Print Services Directive
  - ESDC Privileged Desktop Access Directive
  - ESDC Storage of Electronic Information Directive

Treasury Board

- TB Standard on Email Management (2014)
- TB Policy on Government Security (2019)
- TB Framework for the Management of Compliance (2009)
- TB Policy on Acceptable Network and Device Use (2013)