ESDC Privileged Desktop Access Directive

1. Effective Date and Annual Review

This Directive took effect upon its approval by the ESDC Corporate Management Committee (CMC) on May 13, 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

This Directive informs individuals of the requirements and responsibilities of privileged desktop access and outlines the granting of this access.

4. Basic Requirement

Privileged desktop access is granted only if required by an individual to perform their duties, and where no other reasonable solution exists.

5. Context

5.1 ***Privileged Desktop Access*** provides the account user the ability to install software and hardware and change computer settings on a desktop device.

5.2 The majority of individuals, by default, do not have privileged desktop access; they are restricted to limited changes to personal settings and they cannot install software or hardware.

5.3 Privileged desktop access is granted only on an exception basis because it provides a *privileged* level of access to our network, computers, and information which could expose ESDC to risks that include the installation of unauthorized software, malware, and exposure to hacker attacks.

5.4. Common Reasons for Granting Privileged Desktop Access
Privileged desktop access is required for a variety of reasons, both for ongoing job functions as outlined in Table 4.8, and for temporary requirements such as:

- Registering software
- Temporary help on a project
- Installation of certain specialized software

5.5 There are four types of ESDC network accounts that include privileged desktop access as part of their privileges. They are the *Local Administrator, Workstation Administrator, Security Administrator,* and *Enterprise Administrator* accounts. (See Table 5.8)

5.6 The Local Administrator account provides the individual with privileged access only to their own desktop and is therefore the most widely granted of these privileged accounts.

5.7 The Local Administrator account is granted through the procedure outlined in Section 6.3 of this Directive. Because Workstation, Security, and Enterprise accounts belong to a specific job function, they are provided to individuals as part of their job.

5.8 Table of Administrator Accounts that have Privileged Desktop Access

TYPE OF ADMINISTRATOR ACCOUNT	PRIVILEGED ACCESS TO DESKTOP	USED BY
1. Enterprise Administrator (highest level of privilege)	Full access to all objects in the directory, which includes all desktops.	• A small group in SSC.
2. Security Administrator (second highest level)	Full access to all desktops	• IT Security in ESDC and SSC to support the security toolset.
3. Workstation Administrator (third highest level)	Full access to all desktops	• IITB staff who support desktop services and specific product management functions.
4. Local Administrator (lowest level)	Full access to the local desktop	• Non-technical users for a specified purpose, e.g.to change settings or use software tools that function only with admin rights (usually granted to non-technical users for a specified purpose). • IITB's Shared Application Development Environment (SADE) to configure and support devices in the application development environment and maintain the environment. • Some individuals that require local access to support their job requirements (e.g. Client Service Operations & Solution Development (CSOSD), IITB)). • Some individuals for application specific installation. (A small number of applications require an individual to have Local Administrator privileges on the end-user device in order for the application to function correctly.)

6. Detailed Requirements

6.1 Responsibilities

a) An individual who is granted privileged desktop access must only use these privileges for the specific purposes for which they were approved, as stated in the rationale for these privileges (see section 6.3).

b) Unless otherwise stated in an IITB-approved rationale for privileged desktop access, an individual does ***not*** have the authority to:

- Download or install software of any kind including updates, plug-ins, purchases, trial versions, freeware, shareware, and open source;
- Change a configuration setting that modifies or defeats anti-virus, anti-malware, monitoring or data loss prevention software;
- Install hardware devices of any kind (refer to the Portable Storage Devices Directive);
- Grant privileged desktop access to any other account user.

6.2 Requesting the Installation of Software or Hardware

a) ESDC has a suite of approved software and hardware, and installation processes for both. An individual with privileged desktop access cannot install any software or hardware, unless it is clearly specified as an exception in their approved rationale.

b) If an individual is approved to install software as a part of their work duties (privileged access), prior to installation, they must:

- Verify that the software is on the List of ESDC Approved Standard IT COTS Products and contact the National Service Desk to ensure there are available licences (if applicable).
    - If the software is not on the List of ESDC Approved Standard IT COTS Products, then the individual must submit a request to the National Service Desk in order to for the software to be assessed for use.

6.3 Requesting Local Administrator Privileges

a) Most Local Administrator privileges are granted temporarily, and for a specific approved purpose, while some are granted for specific roles or jobs. Once the approved purpose for which the account was granted has been completed, these privileges must be subsequently revoked.

b) All requests must be signed by the individual, endorsed by the individual's Director, and approved by the individual's Director General (DG). The process for requesting Local Administrator Privileges and closing them can be initiated through the National Service Desk (NSD).

6.4 Management of Privileged Desktop Access

a) Privileged desktop access is associated with the name of the individual who is granted this privilege. The list of account holders will be reviewed annually by IITB and reconfirmation of the requirement will be requested where necessary.

b) When an employee leaves the department, changes positon or no longer requires an Administrator Account, the individual's DG shall advise the National Service Desk to remove the Administrator Account.

7. Monitoring and Reporting

The Department monitors and reports on individuals' activities on the departmental electronic network in order to enforce acceptable use of departmental resources. Improper use of administrator privileges will be reported to management so that appropriate measures can be taken.

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. Enquires

Questions regarding this Directive should be directed to IT Security at NA-ITSCOE-CEMSTI-GD@servicecanada.gc.ca.

10. References

Treasury Board Secretariat

- TBS Policy on Government Security (2019)
- TBS Policy on Acceptable Network and Device Use (2013)

ESDC

- 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

Communications Security Establishment

- Managing and Controlling Administrative Privileges Explained - IT Security Bulletin for the Government of Canada