**Departmental**

**Telework Directive**

Effective May 20, 2016

**Telework Directive**

The effective date of this Directive is May 20, 2016. This Directive replaces the Telework Directive that was effective April 1, 2013.

**Preamble**

Employment and Social Development Canada (ESDC) is committed to fostering workplace well-being and providing policies and programs designed to help employees balance their work, personal and family responsibilities. Telework is one of several flexible work arrangements that may be considered within the context of the employer’s operational requirements and employee needs.

The Telework Directive describes the Department’s commitment to considering telework when appropriate, and the various requirements to be met when approving telework arrangements given the Department’s business context and strategic orientations.

**ESDC Context/Strategic Orientations**

ESDC’s mission is to build a stronger and more competitive Canada, to support Canadians in making choices that help them live productive and rewarding lives, and to improve Canadians’ quality of life. The Department is committed to excellence in all it does and serves Canadians with a focus on respect, accountability and results. ESDC engages employees in this mission, establishes a healthy work environment, nurtures a culture of teamwork, and builds leadership capacity.

ESDC is transforming service delivery approaches to bring significant efficiencies while improving service to Canadians and internal services that support those who serve Canadians. Existing work practices must evolve to fit the new service delivery model and operational context.

In establishing a telework directive, the Department recognizes its primary accountability is to serve Canadians effectively and efficiently, and to continuously review technological advances that would enhance the safeguarding of citizens’ information, in accordance with the [*Privacy Act*](http://laws-lois.justice.gc.ca/eng/acts/P-21/), the departmental Privacy Code and the [Treasury Board of Canada Secretariat’s (TBS) Policy on Government Security](http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578).

This Directive will be reviewed periodically to ensure it is aligned with the departmental mandate, operational changes, and technological advances.

1. **Introduction**

This Directive has been developed in accordance with the [Treasury Board Secretariat`s Telework Policy](http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12559&section=text). It describes the Department`s commitment to considering telework when appropriate and the various requirements to be met when approving telework arrangements. It also sets out a framework for approving and managing telework arrangements and clarifies the elements required to be met by management and employees in order for ESDC to consider telework as an appropriate work arrangement.

The Directive will bring transparency, consistency and clarity to the decision-making and approval processes, and more importantly, will enhance the safeguards put in place by ESDC to ensure the protection and security of the personal information of Canadians.

1. **Objectives**

The objectives of ESDC’s Telework Directive are to:

* Provide guidance and direction to managers when considering telework requests and in implementing effective and cost-efficient telework arrangements;
* Provide guidance to employees when considering submitting a telework request to management;
* Outline the responsibilities and accountabilities of managers and employees with regard to telework;
* Ensure consistency in the application of telework arrangements across the organization;
* Ensure that employees enjoy the flexibility of telework arrangements where appropriate.

**3.** **Application**

This Directive applies to all ESDC term and indeterminate employees, including those in Service Canada and the Labour Program. It does not, however, apply to Labour Program employees who are mobile workers covered by the Mobile Work Framework.

Telework will not be considered for casual employees or students.

For situations requiring a duty to accommodate, refer to [Annex G in the DTA Guidelines](http://iservice.prv/eng/hr/dta/documents/Guidelines_DTA.doc).

**4. Definitions**

**Telework:** Telework is a work arrangement whereby employees have a formal signed agreement with their employer to carry out some or all of their work duties away from the designated workplace. Telework locations can include the employee’s home or another location agreed to in the telework agreement. Telework arrangements are in effect for specific periods of time. Overall length and frequency, including the number of days involved in any potential telework week, must be discussed with, authorized by, and will be subject to annual review by management.

N.B.: Working from home on occasion is not considered to be telework unless it is scheduled and recurring. Nevertheless, proper security measures must be followed and management pre-authorization shall be obtained.

Telework should not to be confused with *hoteling*, which is a temporary arrangement, whereby an employee works from an employer’s premise other than the employee’s designated workplace, for example, a human resources (HR) employee working out of a Service Canada Centre location.

**Designated workplace:** Location of work (i.e. business address) where the employee would perform his/her duties if a telework arrangement was not in place.

**5. Requirements**

Entering into a telework arrangement is at the discretion of management. It is neither a right of the employee, nor an obligation of the Employer.

The approval of each telework situation shall be made on a case-by-case basis at the discretion of management. Participation in a telework agreement is voluntary and employees cannot be required to telework without mutual agreement.

Telework arrangements must ensure, foremost, the protection of citizens’ personal information. As such, managers are required to apply the [Business Risk Assessment Framework (BRAF)](http://iservice.prv/eng/telework/tools_and_resources/docs/business_risk_assessment_framework.docx) for all telework requests for positions involving the handling of citizen information. This will be used to assess the overall risk associated with employees being considered for telework. If employees’ duties do not require the handling of citizen’s personal information, then the BRAF is not necessary.

**When telework may be appropriate**

Prior to entering into a telework arrangement, management must ensure that the following conditions apply:

* It is operationally feasible to perform the work outside of the designated workplace;
* If the position requires the handling of protected citizen information, the employee's duties will be assessed against the BRAF to determine whether the performance of those duties, offsite, are within the limits of the Departmental risk tolerance. Telework may be appropriate if the assessment risk is low to medium;
* The overall quality and quantity of the work carried out in the designated workplace shall be maintained by the teleworker in the telework place;
* Consistency in meeting performance objectives, including adherence to the [Values and Ethics Code for the Public Sector](http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=25049&section=text)*,* and the[ESDC Code of Conduct](http://iservice.prv/eng/is/ve/code_of_conduct/index.shtml);
* The arrangement is cost-effective and the funding is within the approval manager’s budget to support expenses associated with the agreement;
* The employee will be accessible when required by management and colleagues during the employee’s scheduled working hours, and agrees to report to the designated workplace, as necessary, to attend meetings, training sessions, etc, at his/her own expense;
* The arrangement will not negatively impact colleagues’ workload and the achievement of team/task outcomes.

Failure to meet any one of these requirements will result in the denial of the telework request or the termination of the telework agreement in place.

A telework arrangement can be amended or terminated at any time with a four (4) week notice from either party. However, in exceptional circumstances (such as: a security incident, unforeseen operational requirements), the arrangement can be terminated by management without notice.

**When telework will not be considered**

Certain categories of work and situations will not be considered for telework as these do not meet operational requirements and/or pose too high a risk for the safeguarding of information:

* Duties involving on-site, in-person services to citizens (as a substantial part of the duties);
* As calls cannot be dispatched outside the call centres and cannot be monitored or tracked to ensure quality of service and/or distribution of national workload, duties requiring direct citizen contact by telephone will not be considered;
* If the position requires the handling of protected citizen information, the employee's duties will be assessed against the BRAF to determine whether the performance of those duties, offsite, are within the limits of the Departmental risk tolerance. Telework may not be considered if the assessment confirms a high risk; however, the discretion to approve the request remains at the ADM level;
* Positions where consolidation of work sites occurs given that telework does not achieve budget and transformation objectives such as efficiency, effectiveness and workload management;
* Duties requiring the handling of classified information at the protected C, secret or top secret level, as the departmental electronic network is certified up to the protected B level. In addition, this type of information can only be handled in a controlled environment as per the [Policy on Government Security](http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578);
* Duties requiring the handling of sensitive information, levels A and B (paper or electronic format),where the level of risk to the safeguarding of the information requires mitigating measures that are too costly and/or result in too high a residual risk. The judgement on cost and acceptable risk tolerance will be made at the Assistant Deputy Minister level to bring consistency;
* Managers or supervisors whose responsibilities may require their presence in the designated workplace.

[A step-by-step process is included in Annex 1](#annex1)

**6. Roles and Responsibilities**

**Managers and supervisors will:**

* Receive and assess a telework request;
* Ensure that all requirements as described in Section 5 of this Directive, are met;
* Complete the BRAF for any position which involves the handling of citizen’s personal information;
* When handling of Protected Information (Level A and/or B) at the designated telework location:
* Obtain employee’s consent to the conduct of a potential [Threat and Risk Assessment (TRA)](http://iservice.prv/eng/telework/tools_and_resources/docs/tra_assess_checklist.doc) of the proposed telework location (refer to [Employee’s Telework Request Form](http://iservice.prv/eng/telework/tools_and_resources/docs/employee_tw_request_form.docx));
* Consult with the [Regional Security Officer](http://iservice.prv/eng/is/security/contact_us/rso_contacts.shtml) (RSO) of the Internal Integrity and Security Directorate, Integrity Services Branch to initiate a TRA of the telework location;
* To the extent possible, accompany the RSO during the visit to the telework location, when a TRA is required;

Or,

* When handling of unclassified Information:
  + A TRA is not required if there is no handling of Protected Information (Level A and/or B) at the designated telework location;
  + Obtain from the employee the [*Self-Assessment and Attestation Process for the Handling of Unclassified Information*](http://iservice.prv/eng/telework/tools_and_resources/docs/selfassess_handling_info.doc);
  + Attest to the fact that the duties to be performed at the proposed telework site will not include the handling of Protected or Classified Information;
  + Provide the completed *Self-Assessment and Attestation Process for the Handling of Unclassified Information* form to the RSO for review and sign-off;
* Obtain formal approval by the Assistant Deputy Minister (refer to the [*Management Assessment and Recommendation Form*](http://iservice.prv/eng/telework/tools_and_resources/docs/management_tw_assess_form.docx));
* Inform the employee of the decision;
* Monitor telework arrangements;
* Make employees aware of all their duties and responsibilities in telework situations;
* Ensure employees have received appropriate training, including [mandatory training](http://hrsdc.prv/eng/career/effectiveness/index.shtml) prior to commencing telework;
* Report all security incidents to the RSO and complete a Security Incident Report ([ADM 3061](http://forms-formulaires.prv/eform99/index.cfm?App=Launch&FormID=5702&GroupID=25&LANG=E)), as required on all work sites;
* Consult Regional OHS Advisors for additional information on OHS obligations under telework agreements, as required on all work sites;
* Report all OHS incidents in accordance with the “[*If a Work-Related Accident Occurs…*](http://iservice.prv/eng/hr/ohs/topics/if_accidents_occurs.shtml)” procedures;
* Ensure that approved telework agreements are communicated among team members while respecting the employee’s right to privacy;
* Monitor timelines and initiate the renewal of telework agreements prior to their end date to allow sufficient time for the approval process;
* Terminate telework arrangements if required.

**Employees will:**

* Prepare and submit their request for telework as per the step-by-step process in Annex 1;
* Use only department-approved equipment;
* Assume the costs of equipping and maintaining the telework location (such as office furniture, insurance, heat and hydro, telephone, and internet access);
* Ensure that the telework arrangement does not contravene municipal zoning regulations nor the employee’s residential lease, if applicable;
* Ensure that the equipment in the telework location is maintained and meets departmental health, safety, and security requirements or standards (See Section 9, *Reference*s);
* Safeguard documents, assets and equipment as per departmental policies, standards and guidelines (See Section 9, *Reference*s );
* Comply with all terms and conditions of employment, relevant collective agreements, applicable legislation, TBS and departmental policies, at the telework location (See Section 9, *References)*;
* Use supplies, equipment and electronic networks belonging to the employer only for the purposes of carrying out the duties and responsibilities of their position;
* Return all work-related information as and when requested by management;
* Immediately notify the manager if any requirement set out in this Directive or in the Telework Agreement is no longer being met;
* Consent to provide the RSO, or delegated authority with access to the telework site;
* Complete the *Self-Assessment and Attestation Process for the Handling of Unclassified Information* when required, i.e. handling of unclassified information at the proposed telework site;
* Report all security-related incidents to their immediate supervisor/manager and complete the Security Incident Report (ADM 3061), as required on all work sites;
* Agree to maintain a dedicated workspace within the telework location that meets the occupational health and safety requirements, outlined in the [Departmental Occupational Health and Safety Program](http://hrsdc.prv/eng/hrsb/hrs/ohs/index.shtml);
* Report any occupational health and safety hazards within the dedicated workplace and any work-related injuries/illnesses to their immediate supervisor/manager, as required on all work sites.

Notes:

Employees entering into a telework arrangement continue to be subject to the [*Government Employees Compensation Act*](http://laws-lois.justice.gc.ca/eng/acts/G-5/).

**The Human Resources Services Branch will:**

* Provide relevant advice to employees and managers involved in, or wishing to enter into telework arrangements;
* Provide advice on occupational health and safety matters.

**The Innovation, Information and Technology Branch (IITB) will:**

* Provide IT advice to employees and managers involved, in or wishing to enter into, telework arrangements;
* Provide required IT and telecommunications-related equipment and appropriate system access;
* Maintain an up-to-date list of departmental equipment and software utilised by teleworkers;
* Provide technical support to teleworkers during business hours.

**The Regional Security Office (RSO) will:**

* Conduct and assess the Threat and Risk Assessment (TRA) on the proposed telework site when required, i.e. handling of Protected Information (Level A and/or B) at the proposed telework site;

or,

* Review the completed employee *Self-Assessment and Attestation Process for the Handling of Unclassified Information* form when required;
* Provide functional advice to management on the TRA conducted at the telework location and advise management of any deficiencies/concerns that need to be addressed prior to entering into an agreement;
* Determine if a TRA is required when receiving an application for renewal on the basis of considerations such as:
  + change in the employees’ duties/responsibilities;
  + relocation of the telework site or changes to the telework site that could change / influence the initial assessment;
  + change in the number of occupants in the telework site (i.e. new roommate);
  + the existence of security incidents reported during the period of the previous agreement.
* Track and maintain a list of telework agreements by region.

**Assistant Deputy Minister’s Office:**

* Reviews and approves telework requests;
* Informs management of the decision by returning a scanned copy of the signed form with a copy to the [Regional Security Office](http://iservice.prv/eng/is/security/contact_us/rso_contacts.shtml) which is responsible for retaining the list of telework agreements in the region.

**7. Performance Management for Teleworkers**

Managing teleworkers will be conducted in the same manner as managing employees in the designated workplace. The Department’s performance management process will be utilised for setting performance objectives, defining performance measures (expected results) and providing regular feedback to teleworkers.

**8. Accountability and Monitoring**

While telework arrangements must be assessed on a regular basis as part of performance management (i.e. ensuring the quality and quantity of work carried out meet performance expectations), all telework agreements must be reviewed on an annual basis by management to ensure that the requirements outlined in section 5 of this Directive continue to be met.

The duration of the telework agreement must not exceed one year from the date the employee started to telework and can be subsequently renewed.

The RSO will maintain a copy of all telework agreements and TRAs for their respective region (National Capital Regional, Atlantic, Western Canada and Territories, Ontario and Quebec).

IT is responsible for monitoring the use of the network, departmental IT equipment and software utilised by the teleworker.

**9. References**

**Acts, Legislation and Policies**

[ESDC Code of Conduct](http://iservice.prv/eng/is/ve/code_of_conduct/index.shtml)

[Values and Ethics Code for the Public Sector](http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=25049)

[Departmental Occupational Health and Safety Program](http://iservice.prv/eng/hr/ohs/index.shtml)

The [*Access to Information Act*](http://laws-lois.justice.gc.ca/eng/acts/A-1/) and the [*Privacy Act*](http://laws-lois.justice.gc.ca/eng/acts/P-21/index.html)

**ESDC Departmental Security Policies and Procedures**

[ESDC Network Use Directive](http://iservice.prv/eng/imit/catalogue/itsecurity/tools_and_resources/toolkit/network_use_directive.shtml)

[TBS Telework Policy](http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12559)

[TBS Policy on Acceptable Network and Device Use](http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=27122)

[*The Public Service Labour Relations Act*](http://laws-lois.justice.gc.ca/eng/acts/P-33.3/)

[Collective Agreements](http://www.tbs-sct.gc.ca/pubs_pol/hrpubs/coll_agre/siglist-eng.asp)

**Departmental Telework Related Forms**

[Employee Self-Assessment Tool](http://iservice.prv/eng/telework/tools_and_resources/docs/self_assess_against_directive.doc)

[Employee Request Telework Form](http://iservice.prv/eng/telework/tools_and_resources/docs/employee_tw_request_form.docx)

[Telework Agreement](http://forms-formulaires.prv/eform99/index.cfm?App=Launch&FormID=6712&GroupID=144&LANG=E)

[Business Risk Assessment Framework (BRAF)](http://iservice.prv/eng/telework/tools_and_resources/docs/business_risk_assessment_framework.docx)

[Management Assessment and Recommendation Form](http://iservice.prv/eng/telework/tools_and_resources/docs/management_tw_assess_form.docx)

[Guidelines for Conducting Threat and Risk Assessments on Telework Sites](http://iservice.prv/eng/telework/tools_and_resources/docs/guideline_tra.doc)

[Telework Threat and Risk Assessment Checklist](http://iservice.prv/eng/telework/tools_and_resources/docs/tra_assess_checklist.doc)

[Telework Self-Assessment and Attestation Process Form](http://iservice.prv/eng/telework/tools_and_resources/docs/selfassess_handling_info.doc)

[Telework Security Briefing Form (ADM 5019)](http://forms-formulaires.prv/eform99/index.cfm?App=Launch&FormID=57&GroupID=140&LANG=E)

[Loan of Departmental Equipment (ADM 3004)](http://forms-formulaires.prv/eform99/index.cfm?App=Launch&FormID=1180&GroupID=140&LANG=E)

[Return of Departmental Equipment (ADM 5018)](http://forms-formulaires.prv/eform99/index.cfm?App=Launch&FormID=56&GroupID=140&LANG=E)

[Security Incident Report (ADM 3061)](http://forms-formulaires.prv/eform99/index.cfm?App=Launch&FormID=44&GroupID=140&LANG=E)

[Health and Safety Checklist of the Telework Site](http://iservice.prv/eng/telework/tools_and_resources/docs/health_safety_checklist.doc)

**Updated by:** Labour Relations - Centres of Expertise

Human Resources Services Branch

**Date:** May 20, 2016

**or**

Requirements outlined in Section 5 of the Telework Directive would not bet met –

**Do not submit request**

Provide rationale/reasoning to employee

**ADM Review and**

**Approval Process**

1. ADM sign-off on decision.

2. Notify Manager of decision.

3. Provide signed copy of Telework Agreement to RSO.

**No**

1. Request denied.

2. Manager advises employee.

3. Process ends.

**Yes**

Proceed to with completing **Telework Request Form**.

**Yes**

Proceed to next steps.

**No**

Request denied.

**Manager**

1. Ensures all the requirements are met as per Section 5 of the Telework Directive. **Management Assessment and Recommendation form)**

**Process to be completed by Manager**

1.Obtain Employee Telework Request Form duly signed.

2. Determine if the position requires handling of citizen information. If so, proceed with the BRAF. If low to medium risk, proceed with step 3.

3.Initiate a Threat and Risk Assessment (TRA) of telework site with the Regional Security Office (RSO), using the Telework **TRA Checklist**.

4.In collaboration with RSO, ensure that telework site meets departmental security standards.

5.In collaboration with regional OHS advisors, ensure that the telework site meets health and safety standards.

6.Address any or all of the recommendations made by the RSO and/or OHS Advisor regarding any deficiencies found in order to meet security and safety standards.

7.Conduct follow up to ensure that appropriate action has been taken prior to further consideration.

8.Complete the Management Assessment and Recommendation Form and send request including TRA report for ADM review/approval committee.

**Employee**

1. Consents and agrees to the terms and conditions of the telework agreement by completing and signing off on all official forms and documents which includes but is not limited to a security briefing form for the protection of sensitive information and or assets assigned as part of the duties to be carried out in the telework site.

**Yes**

Manager proceeds to next steps.

**Manager**

1. Complete and sign the **telework agreement**.

2. Complete required Telework forms (e.g. Telework Security Briefing form, Loan of Equipment form, etc.)

3. Briefs employee on safety and security requirements and obtains consent on all forms.

4. Provide forms to the appropriate stakeholders.

(Note: Copies of Loan of Equipment forms are to be provided to Assets Management and IT Security for their files. Manager signs off on all forms and maintains copies for office use).

**Telework will include the handling of**

**Sensitive Information**

**Protected - Levels A - B**

**Telework will only include the handling of**

**Unclassified Information**

**Process to be completed by Manager**

1.Obtain Employee Telework Request Form duly signed.

2.Ask the employee to complete the **Telework Self-Assessment and Attestation Process** **(TSAAP)** for the handling of Unclassified Information.

3.Certify and attest to the fact that the duties to be performed by the employee at the telework site will not include the handling of Protected and/or Classified information.

4.Provide the TSAAP form to the RSO, to ensure that telework site meets departmental security standards.

5.In collaboration with regional OHS advisors, ensure that the telework site meets health and safety standards.

6.Address any or all of the recommendations made by the RSO/OHS Advisor regarding any deficiencies found in order to meet security and safety standards.

7.Complete the Management Assessment and Recommendation Form and send request including Telework Self-Assessment and Attestation Process form for ADM review/approval committee.

**Employee completes the**

**Employee Self-Assessment Tool.**

**Employee** may initiate informal discussion with manager on the refusal of the telework request

**Employee** may initiate informal discussion with manager on the refusal of the telework request