



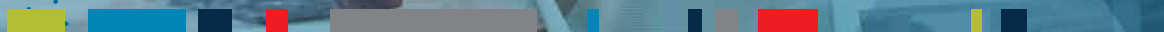
Canadian Security
Intelligence Service

Service canadien du
renseignement de sécurité

UNCLASSIFIED

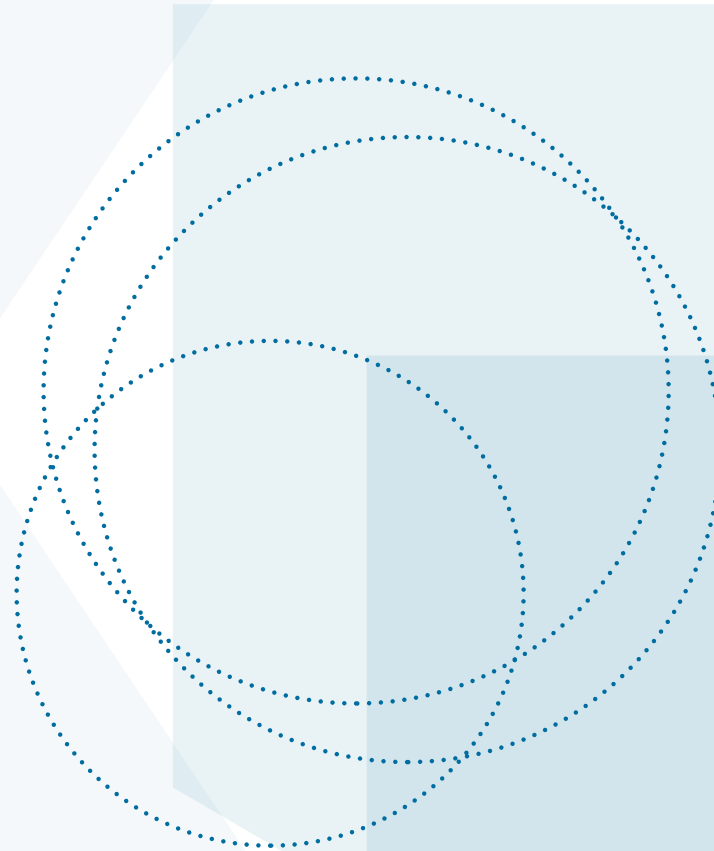


CSIS CODE OF CONDUCT



A SAFE, SECURE AND PROSPEROUS CANADA THROUGH TRUSTED INTELLIGENCE AND ADVICE.

Canada 



/// CLARIFICATION:

Examples, clarifications and tips mentioned throughout the Code are used to provide context, and decrease ambiguity. As the reader you should note that whatever examples, clarifications and tips are given are not exclusive but representative. Always remember to **Stop. Reflect. Inquire.** if you are uncertain or have questions.

TABLE OF CONTENTS

SERVING CANADIANS WITH INTEGRITY	4
OUR COLLECTIVE COMMITMENT	4
OUR VALUES IN ACTION	5
STOP. REFLECT. INQUIRE.	6
CSIS VALUES	8
1. RESPECT FOR PEOPLE	8
2. RESPECT FOR DEMOCRACY	11
3. INTEGRITY	13
4. STEWARDSHIP	14
5. EXCELLENCE	15
BREACH OF CONDUCT	16

SERVING CANADIANS WITH INTEGRITY

OUR COLLECTIVE COMMITMENT

As employees of the Canadian Security Intelligence Service (CSIS, *the Service* or *the organization*), [our mission](#) is to protect Canada's national security interests and the safety of Canadians through trusted intelligence and advice. We take pride in knowing that the work we do makes a difference in the lives of Canadians as we contribute to a safer and stronger Canada. Commitment to the CSIS Code of Conduct is vital to the successful achievement of the organization's goals.

We are committed to providing a healthy and respectful workplace that is free of harassment, discrimination and reprisal, to ensure the health, safety and well-being of employees at all levels. We interact with one another in a positive and respectful way, and we demonstrate our commitment to work with integrity towards our goal of protecting Canada's national security interests and the safety of Canadians. In addition, we are responsible for demonstrating the values of this Code through our behaviours and be guided by them in all activities during the performance of our professional duties.

Adhering to the Code of Conduct is a condition of employment for CSIS employees*, including indeterminate and term, executives, students and casual employees. All are required to review and acknowledge the Code of Conduct on an annual basis. Seconded, intregrees, contractors and service providers are expected to respect the principles and intent of this Code of Conduct and other relevant policy documents as well as abide by the terms and conditions of their agreement with CSIS.

**For unionized employees, should this Code of Conduct conflict or overlap with the provision of the Collective Agreement, the Collective Agreement will take precedence.*

/// MORE INFO:

A measure to promote a healthy and respectful workplace is ensuring that all employees have read and understand the CSIS Code of Conduct (the Code). Accordingly, all employees are required to affirm annually that they have read and understand the following documents: CSIS Code of Conduct, Directive on Conflict of Interest and Post-Employment.

OUR VALUES IN ACTION

The **five values** of our organization, as detailed in this Code, guide direction, enable decision making and inspire behaviour. However, they benefit us only when they are living principles; practiced every day in the workplace and in the work we do for Canadians. These values cannot be considered in isolation from each other as they will often overlap, which means that they are interdependent and mutually reinforcing.



This Code of Conduct assists us to integrate each value into all areas of our work lives, from day-to-day decision making to policy development to operational work, no matter the level or position we occupy. In any decision that we make, it is expected that we consider, discuss and challenge ourselves to uphold these values.

/// FIVE VALUES:

The five CSIS Values are: Respect for People, Respect for Democracy, Integrity, Stewardship and Excellence.

By committing to this Code of Conduct we strengthen the cultural values of the workplace and contribute to building trust among colleagues and public confidence in the organization. Equally, we can expect to be treated in accordance with these values by our colleagues and management.

/// MORE INFO:

Our values define who we are and what is important to us as an organization.

Values are concepts that transcend context. Beliefs, on the other hand, are context-dependent: your beliefs depend on the world views of the culture you were brought up in and the parental programming you received in your formative years.

Although we may not share the same beliefs, values can be used as a tool for creating internal cohesion in an organization. When we declare our values, our workforce, our partners and Canadians know what we stand for.

How do we know if someone is embodying these values as we cannot see them just by looking at a person?

The answer is simple: Observe behaviors. If we, as individuals or an organization at large, are living with integrity, our values will be compatible with our behaviors. It is what we do and how we do it, rather than what we say, that sheds light on who we really are and what is important to us.

STOP. REFLECT. INQUIRE.

CSIS relies on every single employee to embody these values and to speak up when necessary. It counts on our employees to be proactive and seek guidance when they have concerns. The Code of Conduct does not account for every scenario.

In the performance of our duties and functions, employees must comply with Canadian law, including but not limited to, the [*CSIS Act*](#), the [*Canadian Charter of Rights and Freedoms*](#) and the [*Privacy Act*](#), and with Ministerial Directions. Employees must also comply with requirements set out in the *CSIS Governance System* (e.g. policies, procedures). Finally, we must act in accordance with decisions of the Court and comply with terms and conditions set by the Court.

Employees may seek advice from **policy centres** to ensure compliance. Whenever you feel uncertain about a situation, the most important thing to remember is to Stop. Reflect. Inquire.

At CSIS we embrace the diversity of thought and encourage open dialogue. Questions and concerns are important to the organization and we encourage our employees to speak up and voice them respectfully.

The following pages will define each value separately and the expected behaviours that support them. If a particular situation isn't discussed in this Code, it does not change or remove your responsibility to use judgment and integrity when deciding what

to do. If you need help speak with your supervisor or one of the key contacts.

Employees are encouraged to speak with their supervisors first. Should you not feel comfortable in doing so, make use of the various key contacts:

- Employee Assistance Program (EAP);
- Employees' Association / Union Representative;
- Human Resources Services and Regional HR;
- Internal Conflict Management Services (ICMS);
- Internal Security (IS) to report a security concern;
- Labour Relations (LR);
- Psychological Health and Safety Program (PHS);
- Senior Officer for Disclosure of Wrongdoing; and
- Relevant Policy Centre(s).

Employees may also consider consulting with their supervisors' supervisor.

/// POLICY CENTRES:

The policy centres are an organizational unit containing a specialized expertise. They establish corporate policies, standards, procedures and guidelines for the responsibility centres and provide them assistance, service and advice.

DID YOU KNOW?

Our Code establishes principles for business conduct applicable throughout our organization, regardless of location.

If you're working abroad, at a CSIS sponsored conference/training, or at CSIS sponsored events, always remember that you are representing CSIS, the Government of Canada (GC) and Canadians.

STOP. REFLECT. INQUIRE.



CSIS VALUES

1. RESPECT FOR PEOPLE

As employees of CSIS we respect human dignity and the value of every person by:

1.1 Valuing diversity and inclusion, ensuring equitable treatment of all colleagues, clients, partners and stakeholders.

1.1.1 Recognizing the talents, contributions and ideas that members of our workforce generate and recognizing that they are a source of innovation.

1.2 Providing a healthy and respectful workplace that makes every effort to ensure that employees feel valued.

1.2.1 Participating in the resolution of conflict cooperatively and in doing so minimizing its impact on others and the workplace.

1.2.2 Behaving respectfully by listening to others, seeking to understand their position.

1.2.3 Maintaining collaborative working relationships through honest and positive communications free from **violence**, **harassment**, **discrimination**, and **reprisal**, and addressing inappropriate behaviour promptly and cooperatively.

/// VIOLENCE:

Workplace violence constitutes any action, conduct, threat, or gesture towards a person in their workplace that can reasonably be expected to cause harm, injury, or illness.

/// HARASSMENT:

Harassment is improper conduct by an individual, that is directed at and offensive to another individual in the workplace, including at any event or any location related to work, and that individual knew or ought reasonably to have known would cause offense or harm.

/// DISCRIMINATION:

Discrimination is excluding or restricting members of one group from opportunities that are available to other groups based on the following prohibited grounds: race, national or ethnic origin, colour, religion, age, sex, sexual orientation, gender identity or expression, marital status, family status, genetic characteristics, disability and conviction for which a pardon has been granted or in respect of which a record suspension has been ordered.

/// CONSULT:

Informal conflict resolution mechanisms such as coaching, facilitation, and mediation are often helpful in resolving workplace issues, and may prevent a situation from escalating. Confidential and impartial services are available through Internal Conflict Management Services.

If you experience a challenging personal or work-related situation, you can reach out to the Employee Assistance Program for confidential services.



/// REPRISAL:

Reprisal is defined by behaviours and/or actions taken against an individual who, in good faith, seeks advice, raises a concern, reports possible misconduct, or participates in a formal or informal investigative process. Examples of reprisal may include reassignment, demotion or disciplinary action, passing over for a project or promotion, any measure that adversely affects the employee's working conditions, and directly or indirectly threatening any of the above. Reprisal can also be small, subtle decisions that may be cumulative and finally result in the marginalization of an employee.

1.3 Protecting the physical and psychological health and safety of every employee in the workplace by following health and safety regulations.

1.3.1 Promptly reporting when there is a threat or any work-related hazard, accident or injury to ourselves or other employees.

/// PROMPTLY REPORTING:

Depending on what the work-related hazard is, employees should promptly report issues to the corresponding policy centre including but not limited to Internal Security and the Workplace Health and Safety Committee.

1.4 Contributing to a workplace that is free of any form of reprisal.

CSIS will not tolerate reprisal of any kind against anyone who, in **good faith**, seeks advice, raises a concern, reports possible misconduct, or participates in the investigation of a report or complaint. Reprisal can take either **work** or **social** form and can be reported in the following ways:

- Your manager;
- Your supervisors' supervisor;
- Your DG;
- Your EA/Union representative; or
- Labour Relations (LR).

/// GOOD FAITH REPORTING:

An individual is considered to have reported in good faith if they have brought forward the complaint or participated in providing information during an investigation, based upon a reasonable belief that the information provided is true.

/// WORK:

Work-related reprisals include unsupported negative performance evaluations or disciplinary actions, arbitrary denial of promotions or other job benefits and unfounded reduced or limited work assignments.

/// SOCIAL:

Examples of social reprisal include: Discrimination or harassment from co-workers and/or supervisor; intimidation or humiliation, derogatory remarks or social isolation which occur indirectly or directly; physical threats and/or destruction of property.

DID YOU KNOW?

As a leader, including executives, managers, supervisors and team leads at CSIS you have a network to assist and support you in your duties and functions. Some of these include but are not limited to:

- HR Advisory Panel
- most answers can be found here for supervisors in need of support;
- Supervisor Training and other leadership development training;
 - Manager's Minute;
 - Mentoring; or
 - Any of the key contacts listed.

As a leader at CSIS you are required to make decisions that can affect a variety of people.

Should you have questions or concerns

Stop. Reflect. Inquire.

/// MORE INFO:

The goal of the HR Advisory Panel (comprised of Labour Relations, Psychological Health and Safety, Occupational Health and Safety, Internal Conflict Management Services, Employees Association, Performance Management and Union) is to provide supervisors and managers tools and resources to effectively manage issues in the workplace.

1.5 Modelling our values on a daily basis through applied **ethical leadership** and decision making. Leaders (including executives, managers, supervisors, team leads, and anyone in a position of influence) are required to demonstrate these values, and create healthy and respectful workplaces to enhance and support employee well-being and productivity.

/// ETHICAL LEADERSHIP:

Ethical leadership means guiding your people, leading by example, and doing the “right thing” without abandoning your organizational values.

1.5.1 As a supervisor, manager or executive at CSIS, you are required to:

- create and sustain a work environment that guides, enables, and inspires employees to adopt and carry-out the values of this Code.
- set an example for others by leading ethically, aligning your actions with the values and standards of this Code and the Directive on Conflict of Interest and Post-Employment;
- foster learning by offering advice and guidance, when appropriate, and encourage values-based discussions;
- manage employee performance by establishing clear work objectives, providing regular feedback and formally holding two-way discussions;

- make sure the employees you supervise have the training and tools to follow this Code;
- understand and strictly enforce zero-tolerance on reprisal; and
- Take appropriate action to address incidents of unacceptable behaviour.

/// CONSULT:

Learning and Development and Talent Management have a number of resources available, including training that can help you develop, refine or augment your leadership competencies regardless of whether or not you occupy a formal supervisory role.

2. RESPECT FOR DEMOCRACY

As employees of CSIS we respect all Canadian laws and acts and uphold the Canadian parliamentary democracy and its institutions by:

2.1 Serving the public interest in *good faith* and being accountable for any decisions and/or actions while on duty.

/// ACTING IN GOOD FAITH:

An individual is considered to have acted in good faith if they have made a decision and/or taken action with the intent of complying with the CSIS Act and the requirements set out in CSIS Governance System to the best of their abilities at the time.

2.2 Maintaining political neutrality in the performance of our duties, supporting our Minister and respecting the authority of the government in power.

2.2.1 Respecting the Oaths or Affirmations of Allegiance, of Office and of Secrecy.

2.2.2 Carrying out our duties and functions in a non-partisan and objective manner.

2.2.3 Aligning our efforts and expertise with the Government of Canada and CSIS's strategic priorities.

2.3 Enacting the lawful decisions of leaders and carrying out duties in accordance with Ministerial direction, the *CSIS Act* and the organization's policy documents.

2.3.1 Providing impartial, objective and factual information, advice and support to further the CSIS objectives.

2.3.2 Contributing to a compliant culture in which compliance acts as an enabler for our operational activities. Compliance means doing our work lawfully and with integrity.

2.3.3 Searching and providing all relevant documentation requested by Canadians and internal/external bodies when directed. Employees will not destroy, alter, falsify or conceal documents with the intent of denying access.

2.4 Acting respectfully by keeping discussions about CSIS-related issues within the organization, rather than airing them in public or with domestic or international partners and foreign government representatives. Acknowledging that only authorized spokespersons can issue statements or make comments about CSIS's position on any given subject. Be cautious when making comments in public spaces (including on social media fora) when referencing CSIS, so as not to be misconstrued as representing the organization position.

/// MORE INFO:

The *CSIS Act* protects employees who, for the purpose of **lawfully** performing their duties and functions (pursuant to s. 18.2 or s. 20.1), may be required to act in a manner that is not consistent with Canadian laws or the Code of Conduct in order to maintain operational security (e.g. Cover Operations). Should you have questions or concerns **Stop. Reflect. Inquire.**

/// TIP:

When balancing our right to freedom of expression with the importance of duty of loyalty to our employer and impartiality of CSIS, we should consider the following:

- the nature of our official duties;
- the visibility of our position within CSIS and the Public Service;
- the object of the criticism or public statements i.e. is it critical of a policy, directive or program of CSIS? Of another department?; and
- the impact of our action and/or criticism i.e. could it put into question our impartiality or objectivity as a CSIS employee.

2.4.1 Refraining from making public criticisms of CSIS and/or the GC (including posting critical comments on social media fora) while in our role as a Government of Canada employee.

2.4.2 Participating in online activities requires CSIS employees to:

- be mindful of the duty of loyalty, secrecy and non-partisanship;
- be aware of the safety and security of ourselves, our colleagues and operations;
- refrain from disparaging CSIS, its employees and the Government of Canada;
- refrain from discussing work-related issues, problems or matters;

2.4.3 Expressing our opinions as Canadian citizens about issues of the day, as long as those expressions do not negatively impact our ability to perform our duties as CSIS employees, or puts anyone or anything at risk.

DID YOU KNOW?

Participating in online activities not only compromises you personally, but poor online habits may place organizational and national security at risk.

Should you have questions or concerns **Stop. Reflect. Inquire.** For more information consult Internal Security for guidance.



DID YOU KNOW?

CSIS provides information to a number of internal/external bodies including:

- **Information Commissioner (i.e. ATI requests)**
- **National Security and Intelligence Committee of Parliamentarians (NSICOP)**
- **National Security and Intelligence Review Agency (NSIRA)**

External Review and Compliance (ERC) receives reports of any possible unlawful activity or operational non-compliance in the context of the performance of duties and functions of CSIS. ERC also provides support, coordination and communication on operational compliance. **ERC does not assess compliance with the Code of Conduct.** The CSIS Procedures: Reporting of Operational Non-Compliance and Unlawful Activity contain provisions to ensure any matters relating to Breach of Conduct are referred to Labour Relations, Health and Workplace Management.

3. INTEGRITY

As employees of CSIS we serve the public interest by:

3.1 Upholding the highest professional standards, and acting at all times in a manner that will conserve and enhance public confidence in CSIS.

3.1.1 Ensuring that our actions and decisions are free from favouritism, bias or self-interest.

3.2 Respecting and obeying the law, ensuring that our professional and personal activities are lawful and do not affect our performance, our duties or discredit CSIS.

3.3 Making accurate statements or reports.

3.4 Accessing information only if it is required to perform our duties with proper authorization as part of the “need-to-know” principle of CSIS.

3.5 Refraining from using our roles, CSIS property or assets, and non-publicly accessible information to gain personal advantage or to advantage or disadvantage others.

3.5.1 Safeguarding information by classifying, storing and disposing information in accordance with CSIS policy documents.

3.6 Using discretion when referring to our employment with CSIS and maintaining our safety and cover as necessary and that of our colleagues.

3.7 Performing our duties reliably and in compliance with the security clearance we have been granted.

3.8 Respecting Service requirements in relation to the Directive on Conflict of Interest and Post-Employment.

3.8.1 Ensuring that any conflict between our private interests and official duties is always resolved in favour of the public interest.

DID YOU KNOW?

As employees of CSIS, we have the privilege of holding an Enhanced Top Secret (ETS) clearance. One of the responsibilities that come with holding an ETS clearance is that it has to be renewed on a quinquennial basis by Internal Security. As part of the renewal process, you are required to answer a series of questions, which includes having to disclose any involvement in unlawful activities, to assess your reliability, loyalty and reliability as it relates to loyalty.

/// CONSULT:

CSIS policy and procedure on the Management of Information for more details.

CSIS Policy: Protection of Employees/Contractors for more information on safeguarding employees from risks that could arise during the course of your work.

/// TIP:

When in doubt about how to treat specific information **Stop. Reflect. Inquire.** and speak with your supervisor.

DID YOU KNOW?

That in addition to having ownership in the management of your identity, CSIS employees are expected to protect the identity of their colleagues.



4. STEWARDSHIP

As employees of CSIS we use resources responsibly by:

4.1 Investing in the employees of CSIS as our main and most important resource. Supporting the development of skills and competencies.

4.2 Ensuring we use CSIS resources responsibly with the appropriate approvals and accountabilities.

4.2.1 Avoiding waste and misuse of government funds and assets, using them only in our official duties and not for personal gain or use.

4.2.2 Reporting all lost, stolen or damaged assets immediately to our supervisor.

4.2.3 Returning all CSIS assets when we leave the organization or when requested by a proper authority.

4.3 Safeguarding classified information, sharing knowledge as appropriate, and making every effort to uphold security standards of classified information.

4.3.1 Assigning proper levels of classification and physical safeguarding (i.e. where and how we store our information) of all CSIS information.

DID YOU KNOW?

Having delegation of authority (financial and/or in matters of human resources) means you must carry out your authorities in accordance with the [CSIS Act](#), applicable legislation, and policy documents. You are accountable for your authorizations, and must understand the requirements and responsibilities associated with your delegated authorities.



/// MORE INFO:

CSIS resources include:

- Physical and consumable assets (i.e. workstations, blackberries, fleet vehicles/gasoline, office stationary);
- Government funds (i.e. cash, per diems, corporate credit cards);
- Intellectual property (i.e. technologies built/designed by CSIS) Intellectual property is anything we create, design, develop or produce as part of our job. These become property of CSIS and the Government of Canada ; we therefore cannot market or sell any of this property as it is a conflict of interest;
- Human Resources (i.e. our people, hours of work); and
- Information (i.e. access and use of CSIS systems/ databases/networks to view or obtain classified information).

/// TIP:

In an effort to minimize the present and long-term effects that our actions have on people and the environment we should make every effort to consider the value of stewardship and values-based decisions to maximize their potential and use.

5. EXCELLENCE

As employees of CSIS we demonstrate professional excellence by:

5.1 Being reliable and committed to working professionally and collaboratively with our colleagues and partners in our role of protecting the national security of Canadians.

5.1.1 Adopting respectful behaviour and language that reflect the professional image of CSIS and the Government of Canada.

5.1.2 Adapting to changing needs by continuously striving to improve policies and programs.

5.2 Abiding by the terms and conditions of employment.

5.2.1 Reporting fit to work and remaining fit to work at all times in accordance with the Substance Use Directive.

5.3 Providing respectful and professional service.

5.4 Respecting both official languages in accordance with the [*Official Languages Act*](#).

5.5 Creating and maintaining a work environment that encourages collaboration, learning and innovation.

/// MORE INFO:

The value of Excellence requires us all to challenge the status quo, manage risk responsibly and innovate when we see opportunity.

/// TIP:

Demonstrating professional excellence requires us to be aware of what is going on at CSIS. You should be familiar with the general messaging that is communicated on a daily basis.



BREACH OF CONDUCT

As employees we share an obligation to protect and strengthen our workplace culture by never ignoring, concealing or condoning misconduct, and by respectfully challenging behaviour that does not reflect CSIS values. Anyone who suspects, with reasonable grounds and in *good faith*, or has witnessed a breach of conduct is responsible for reporting it through the appropriate channels. Employees who become aware of a potential breach of conduct must inform their supervisor, their supervisor's supervisor or their Director General.

A breach of conduct occurs when an employee violates the expected standards of conduct as set out in applicable legislation, policy documents, the CSIS Policy Framework and/or the Code of Conduct. A breach of this code could result in disciplinary action.

Adherence to this Code of Conduct is a condition of employment for all Service employees. Accordingly, all employees are required to affirm annually that they have read and understand the Code of Conduct. Failure to abide by the Code may result in disciplinary measures, up to and including termination of employment. For additional information, please consult the Directive on Discipline, the Breach of Conduct procedures and the CSIS Disciplinary Measures Guidelines.

