HUMAN RESOURCE SECURITY STANDARD

Information Security Branch
Office of the CIO, Province of BC

Document Version: 1.0
Published: September 2019
Table of Contents

I  INTRODUCTION, SCOPE, BACKGROUND .................................................................3

II  GLOSSARY, TERMS AND DEFINITIONS, LIST OF COMMONLY USED REFERENCES .........................3

1  HUMAN RESOURCE SECURITY ........................................................................4
   1.1 PRIOR TO EMPLOYMENT ........................................................................4
   1.2 DURING EMPLOYMENT ...........................................................................6
   1.3. TERMINATION OR CHANGE OF EMPLOYMENT ..............................................8
I Introduction, Scope, Background

This standard is designed to be read in conjunction with the Information Security Standard (version 2.0) as it is a sub-section or sub-standard of the Information Security Standard (version 2.0) (published here: IM/IT Standards).

II Glossary, Terms and definitions, List of commonly used references

To avoid repetition of content, please check the “Glossary”, “Terms and definitions” and “List of commonly used references” sections of the Information Security Standard (version 2.0) (published here: IM/IT Standards) for the terms and definitions used in this standard.
1 Human Resource Security

This chapter identifies the information security requirements for employees that have an employment relationship with government organizations. To reduce information security risks, the terms and conditions of employment must establish expectations for the protection of government assets, information and services.

This chapter references the terms and conditions set by the BC Public Service Agency for employees and identifies the conditions for external personnel such as contractors.

Supervisors and employees have different security responsibilities and liabilities that apply prior, during, and at the time of termination of employment. Prior to employment, emphasis is on the awareness of expected roles and responsibilities, the screening of prospects and the existence of agreements. During employment, policies establish Supervisor responsibilities, education, training and formal processes to handle problematic security situations. This chapter also establishes rules to ensure a secure transition when employment is ended or changed.

1.1 Prior to employment

1.1.1 Employee security screening must be performed prior to entering a working relationship with the Province.

a) Screening for employees

b) Screening for contractors

Purpose: To verify employment qualification claims made by prospective employees.

1.1.1 a) Screening for employees

The process for employee screening is detailed in BC Public Service Agency Human Resource Policies.

1.1.1 b) Screening for contractors

The process for contractor screening is detailed in Core Policy and Procedures Manual, Chapter 6 – Procurement.

Guidelines:

The process for contractor screening can be used to screen other individuals such as volunteers.

Applicants should be screened to assess their education, skills, knowledge, experience and past work performance. The screening should also confirm the applicant’s identity. The extent of the screening process should be commensurate with the sensitivity of the information and nature of work to be performed.

Ministries may exempt applicants from the screening process where:

- Employees have been previously screened for similar types of government work within the last 2 years; or,
• The sensitivity of the information and nature of work to be performed does not warrant a complete screening process.

Ministries should maintain a list of contractors and other individuals who have been screened and the dates.

**Recommended Tests:**

*Note: 1.1.1 is reported on as part of the annual information security review.*

• Demonstrate that the provisions in the BC Public Service Agency Human Resources Policies, Security Screening have been followed.

• Demonstrate candidates for employment have confirmation of academic and professional qualifications.

### 1.1.2 The terms and conditions of employment must document the responsibility of employees for information and information systems security.

#### a) Terms and conditions of employment

The terms and conditions of employment are defined in the BC Public Service Agency, Human Resource Policies, the Oath of Employment and the Standards of Conduct.

The terms and conditions of employment defined in contracts must include:

• Legal responsibilities and rights (e.g., laws relating to intellectual property rights, freedom of information, and privacy);

• Confidentiality requirements that include responsibilities for the handling and storage of information assets; and,

• Consequences of failing to adhere to the terms and conditions.

#### b) Communication of terms and conditions of employment

Supervisors must ensure terms and conditions of employment are agreed to by employees prior to employment or provision of services, including signing the Oath of Employment and receiving a copy of the Standards of Conduct.

#### c) Violation of terms and conditions of employment

Employees in violation of the terms and conditions of employment are subject to disciplinary action including dismissal, cancellation of contract or other legal remedies.

**Recommended Tests:**

*Note: 1.1.2 is reported on as part of the annual information security review.*

• Demonstrate that employment agreements reflect information security responsibilities.

• Demonstrate contractors are made aware of information security responsibilities.
• Demonstrate that the responsibilities for information and information systems security are included in the employment terms and conditions.

1.2 During employment

<table>
<thead>
<tr>
<th>1.2.1</th>
<th>Supervisors must ensure employees comply with information security policies and procedures.</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) Supervisor responsibilities</td>
<td></td>
</tr>
<tr>
<td>b) Review of security roles and responsibilities</td>
<td></td>
</tr>
</tbody>
</table>

**Purpose:** To establish Supervisor responsibilities for ongoing support and implementation of information security.

1.2.1 a) Supervisor responsibilities
Supervisors must support the implementation of information security policies and practices by:
• Ensuring employees are informed of information security roles and responsibilities prior to being granted access to information or information systems;
• Supporting and encouraging employees to adhere to information security policies; and,
• Requiring that employees conform to the terms and conditions of employment, including information security policies.

1.2.1 b) Review of security roles and responsibilities
Information security roles and responsibilities must be reviewed when staffing or restructuring public service or contract positions, or when implementing new, or significant changes to, information systems.

**Guidelines:**
Supervisors should annually review and validate information security roles and responsibilities in job descriptions, standing offers, contracts and information usage agreements.

**Recommended Tests:**
*Note: 1.2.1 is reported on as part of the annual information security review.*
• Demonstrate that employees are provided guidelines stating information security expectations.
• Demonstrate that awareness programs are provided on information security roles and responsibilities.
• Demonstrate that any contracts not using the General Services Agreement express the requirement to abide by government policy.
• Demonstrate Supervisors ensure that employees participate in mandatory and ongoing information security awareness and training opportunities (e.g., Public Service Agency courses, Security Days).
1.2.2 Employees must receive appropriate information security training and be informed of changes to information security policy and practices.
   a) Orientation for new employees
   b) Ongoing information security awareness, education and training

**Purpose:** To increase employee awareness and understanding of security threats, risks and concerns and information security policies and procedures.

1.2.2 a) Orientation for new employees
Supervisors must include an information security awareness component in orientation processes that employees must complete prior to accessing information or information systems.

1.2.2 b) Ongoing information security awareness, education and training
Supervisors must provide ongoing information security awareness, education and training, addressing topics including:

- Protection of information;
- Information privacy requirements;
- Records management;
- Known information security threats;
- Legal responsibilities;
- Information security policies and directives;
- Reporting information security events;
- Appropriate use of government resources;
- Technology training;
- Information on disciplinary processes; and,
- How to obtain security advice.

**Guidelines:**
Resources on information security awareness, education and training are available from:

- Ministry Information Security Officers;
- Ministry Privacy Officers;
- Corporate Information and Records Management Office;
- The Chief Information Security Officer, OCIO; and,
- Awareness section of the Information Security Branch, OCIO.

**Recommended Tests:**
*Note: 1.2.2 is reported on as part of the annual information security review.*

- Demonstrate an information security awareness program is in place, is active and has wide participation.
- Demonstrate that employees are delivered regular awareness education in their program areas of responsibility.
- Demonstrate Executive level support for information security awareness training and education.
1.2.3 Security breaches or policy violations caused by employees must be reviewed by Supervisors.

a) Reviewing security breaches and policy violations

Purpose: To ensure a process is in place to review the activities of employees who commit an information security breach or policy violation.

1.2.3 a) Reviewing security breaches and policy violations
Upon receipt of information identifying employees responsible for a potential or actual security breach or policy violation, Supervisors are responsible for:

- Ensuring the Ministry Chief Information Officer has been informed of the outcome of the security incident and investigation;
- Assisting in an investigation and verifying the details of the security breach or policy violation;
- Determining, in consultation with the BC Public Service Agency, if disciplinary action is warranted for employees; and,
- Arranging for permanent or temporary removal of access privileges when appropriate.

Recommended Tests:
Note: 1.2.3 is reported on as part of the annual information security review.

- Demonstrate that Supervisors are aware of the procedures required to report security incidents to the Office of the Government Chief Information Officer.
- Demonstrate that appropriate steps are taken to preserve forensic evidence for investigators.

1.3. Termination or change of employment

1.3.1 Responsibilities for employment termination must be documented.

a) Termination of employment responsibilities

Purpose: To ensure information security responsibilities upon termination of employment are defined and assigned.

1.3.1 a) Termination of employment responsibilities
Supervisors must advise employees of ongoing confidentiality responsibilities that continue to apply after termination of employment, as outlined in the Standards of Conduct.

Recommended Tests:
Note: 1.3.1 is reported on as part of the annual information security review.

- Demonstrate that employees have been made aware of confidentiality requirements following termination.