JUSTIN ACCESS AND SECURITY COMMITTEE

Do you use JUSTIN at work?

A Guide for Organizations with Electronic Access to JUSTIN

This Guide is distributed for the use of organizations that have been permitted electronic access to JUSTIN.

Table of Contents

Who should use this Guide?

This Guide is for the use of organizations that have been permitted electronic access to JUSTIN.

Why should you read this Guide?

This Guide provides an overview of what organizations need to know about how the JUSTIN Electronic Access Policy affects them on a day-to-day basis.

The JUSTIN Electronic Access Policy applies to all organizations that have been permitted electronic access to JUSTIN.

When your organization was given electronic access to JUSTIN, your representative signed an electronic access agreement. In that agreement, your organization agreed that it would adhere to all applicable policies, procedures and standards in the JUSTIN Electronic Access Policy, as amended from time to time.

Purpose of this Guide

The purpose of this Guide is to provide organizations with a tool that explains the key features of the 4 electronic access policies that have the most significant impact on organizations that use JUSTIN.

This Guide it is not an overview of all of the JUSTIN electronic access policies. The JUSTIN Electronic Access Policy and Procedures Manual contains a number of policies governing electronic access to JUSTIN that are not discussed in this Guide as well as other background information about JUSTIN. You can read the JUSTIN Electronic Access Policy and Procedures Manual online at: http://www.ag.gov.bc.ca/courts/manuals/justin/.

Key features of the 4 policies that affect organizations with electronic access to JUSTIN on a day-to-day basis

Introduction

The 4 JUSTIN Electronic Access policies that have the most significant effect on organizations on a day-to-day basis are:

1. Security for Electronic Access to JUSTIN
2. Audit Trails and Audits for Electronic Access to JUSTIN
3. Unauthorized Use of Electronic Access to JUSTIN, and
4. Revoking Electronic Access to JUSTIN.

This section of the Guide outlines the key features of these 4 JUSTIN Electronic Access policies but it **does not replicate them in their entirety** from the JUSTIN Electronic Access Policy and Procedures Manual.

Your organization **must** refer to the complete version of these policies found in the JUSTIN Electronic Access Policy and Procedures Manual when taking any action pursuant to them.

#1 Security for Electronic Access to JUSTIN

JUSTIN contains sensitive criminal justice information. A breach of JUSTIN security could result in harm including compromising public safety and the administration of justice.

Every organization with electronic access to JUSTIN is responsible for maintaining the required security in accordance with JUSTIN policy and standards.

Responsibilities of an organization

Organizations will ensure that its users undergo a security clearance as specified by the *Security for Electronic Access to JUSTIN* policy and maintain proof of the clearances being conducted

- A security clearance means, at a minimum, a criminal record name check. Depending upon the information that an employee has access to in JUSTIN, a security clearance may include a more comprehensive background check as well. An employee's consent is required for any type of security clearance and they must be advised of the type of security clearance that their work requires before one is conducted.

- The type of security clearance required for an organization's users is usually explained to organizations when the electronic access agreement for electronic access to JUSTIN is drafted. If you are not sure what the current security clearance requirements are for your employees, please contact the JUSTIN Access and Security Committee at AGCSBJACSCommittee@gems7.gov.bc.ca .

Organizations will ensure that the workstations for JUSTIN-enabled computers are secure as specified by the *Security for Electronic Access to JUSTIN* policy

- It is the responsibility of your organization to ensure that the central processing unit and network connection for each JUSTIN-enabled computer is secured against physical access by the public or non-designated personnel.

- Your organization may be required to install anti-virus detection and repair software on your workstations.

Organizations will report and respond to security incidents as specified by the *Security for Electronic Access to JUSTIN* policy

- It is the responsibility of organizations with electronic access to JUSTIN to establish and communicate to all JUSTIN users the procedures for reporting any breaches of security in the workplace.

Organizations will develop and implement disciplinary processes to respond to unauthorized use of electronic access by employees and contracted workers

- It is likely that your organization already has processes in place for responding to incidents where an employee breaches their employment agreement. If not, the *Security for Electronic Access to JUSTIN* policy requires that all organizations with electronic access to JUSTIN develop and implement formal disciplinary processes for dealing with JUSTIN users who have engaged in unauthorized use of electronic access.

Organizations will train employees and contracted workers so that they have a clear understanding of their role and responsibilities as they relate to security and electronic access to JUSTIN

- It is the responsibility of your organization to ensure that your JUSTIN users understand their role and responsibilities as they relate to security and electronic access to JUSTIN. This includes informing JUSTIN users that they:
    - will not leave their terminal unattended when logged-on to JUSTIN, and
    - will terminate active sessions when they are finished unless they can be secured by a locking mechanism such as a password protected screen saver.

#2 Audit Trails and Audits for Electronic Access to JUSTIN

JUSTIN automatically creates audit trails of JUSTIN usage; this is to protect the information in JUSTIN by ensuring that JUSTIN users are accountable for their use of electronic access. This means that whenever a JUSTIN user creates, modifies or deletes information in JUSTIN this can be traced through their username. Some, but not all, viewing of information in JUSTIN also creates an audit trail.

Compliance Audits

From time to time compliance audits will be conducted to help keep JUSTIN secure. A compliance audit may be carried out on:

- a type of information (e.g. witness names)
- a group of users (e.g. Crown Counsel), or on
- a particular organization.

The purpose of a compliance audit is to ensure that all access and use of JUSTIN is authorized. A compliance audit does not target individual users.

Targeted Audits

A targeted audit may be carried out on:

- one or more JUSTIN users, or a category of users (e.g. all JUSTIN users that submit reports to Crown Counsel), when there is a suspected or confirmed unauthorized use of electronic access, or on
- an organization when there is a suspected or confirmed systemic problem with unauthorized use of electronic access.

Responsibilities of an organization

If your organization suspects or confirms an unauthorized use of electronic access by one of your JUSTIN users, you may request that a targeted audit be done on that person's use of JUSTIN. The procedures for doing this are outlined in the JUSTIN Electronic Access Policy and Procedures Manual in the *Audit Trails and Audits for Electronic Access to JUSTIN* policy.

What could happen to an organization

Your organization may be the subject of a compliance audit.

#3 Unauthorized Use of Electronic Access to JUSTIN

Unauthorized use of electronic access to JUSTIN is serious; JUSTIN contains sensitive criminal justice information. If unauthorized use of electronic access to JUSTIN occurs, it could result in harm, including compromising public safety and the administration of justice.

The *Unauthorized Use of Electronic Access to JUSTIN* policy defines 'unauthorized use' and explains what will happen if a JUSTIN user is suspected of unauthorized use of JUSTIN.

The *Unauthorized Use of Electronic Access to JUSTIN* policy applies to intentional unauthorized use; it does not apply when a JUSTIN user makes a data entry error or accesses information inadvertently due to inexperience or human error.

The *Unauthorized Use of Electronic Access to JUSTIN* policy requires that your organization will advise its JUSTIN users that any unauthorized use of electronic access may result in suspension or revocation of their electronic access privilege or other disciplinary action.

What is an 'unauthorized use' of electronic access to JUSTIN?

An unauthorized use is defined in the policy as including:

creating, viewing, modifying, using, disclosing or deleting information beyond the scope of the permitted access, or for an unauthorized purpose

Example: a JUSTIN user has the authority to modify an accused's name (e.g. to correct a spelling error) but instead intentionally modifies an accused's name so that a search against the real name produces no results.

Example: a JUSTIN user views information that they have the authority to view but then discloses what they have seen to someone in a social context, e.g. a JUSTIN users tells an acquaintance about someone else's criminal record.

electronic access by an authorized user during the course of carrying out their duties that is not a legitimate work-related use consistent with the conditions of employment or terms of contract

Example: while at work, a JUSTIN user goes into JUSTIN to see whether a social acquaintance has a criminal record.

Example: while at work, a JUSTIN user goes into JUSTIN to see what new developments there may be in an interesting or high profile criminal case.

violating the terms of the Account Access Form including:

- **divulging, sharing or compromising a password**

  Example of 'divulging': a JUSTIN users tells someone their password.

  Example of 'sharing': a JUSTIN user logs on to JUSTIN and then allows another person to access JUSTIN under their username/password

  Example of 'compromising': a JUSTIN user writes their password somewhere where another person can access it easily.

- **using another individual user's username**

  Example: a JUSTIN user logs onto JUSTIN using another person's username/password.

  Example: one JUSTIN user logs on to JUSTIN then another JUSTIN user accesses JUSTIN under that person's username.

What happens when you suspect that unauthorized use has occurred?

NOTE: the information outlined below is not comprehensive and is not intended to replace the information contained in the Unauthorized Use policy. **You must refer to the *Unauthorized Use of Electronic Access* policy for the full text of the policies and procedures for responding to unauthorized use of electronic access to JUSTIN.**

Responsibilities of an organization

An organization may report suspected unauthorized use prior to an investigation

- Organizations are not required to report a suspected unauthorized use pending an investigation if the information in question is under the authority of the organization. In any other situation, you must report the

unauthorized use as outlined in the *Unauthorized Use of Electronic Access to JUSTIN* policy.

An organization <u>will</u> investigate all cases of suspected unauthorized use

- Your organization must ensure that all suspected unauthorized use of JUSTIN is investigated. The investigation may be conducted by your organization or you may request assistance from Information Technology Services Division or another organization. As indicated above in the *Audit Trails and Audits* policy, you may also request a targeted audit as part of your investigation.

- 'Investigation' is not defined in the policy. An investigation may be as simple as you noticing that one of your employees is sharing their username and taking the time to review the access policy with them; it may also be as complex as a full criminal investigation. The nature and extent of the investigation depends on the unauthorized use that you suspect.

An organization <u>will</u> decide whether to suspend staff - prior to an investigation - when an unauthorized use is suspected

- If you suspect one of your JUSTIN users of an unauthorized use of JUSTIN, you must decide whether to suspend their access to JUSTIN pending the investigation. The *Unauthorized Use of Electronic Access to JUSTIN* policy sets out the criteria that you will consider when making this decision.

- Information Technology Services Division, Ministry of Attorney General and Ministry of Public Safety and Solicitor General has the authority to immediately suspend the electronic access of an organization's employee, pending an investigation, if the suspected unauthorized use

presents an immediate and substantial risk of harm to JUSTIN.

An organization will report its decision to suspend an employee or contracted worker prior to an investigation

- The *Unauthorized Use of Electronic Access to JUSTIN* policy sets out who you will report the suspension to and what information to provide.

An organization will determine the appropriate action to take once an unauthorized use is confirmed

- If your investigation concludes that an unauthorized use did not occur, the matter is closed.
- If your investigation concludes that an unauthorized use did occur, then your organization will take appropriate action pursuant to the JUSTIN Electronic Access Policy and your organization's own policies and procedures.
- Appropriate action may include suspending your employee's electronic access for a specified period of time, changing their type of access, revoking their access or any action that is permissible under the terms and conditions of their employment.

An organization will report the results of the investigation

- You must report the results of the investigation to the Chair of the JUSTIN Access and Security Committee as well as to a number of other organizations. Please refer to the *Unauthorized Use of Electronic Access* policy for the full text of the policies and procedures for reporting unauthorized use of electronic access to JUSTIN.
- The JUSTIN Electronic Access Policy lists what information must be included when reporting the results of an investigation. When you prepare the report on the results of your investigation, use the format shown on page

15. The Investigation Report for unauthorized use template is online at http://www.ag.gov.bc.ca/courts/criminal/justin.

An organization may request a review of an investigation done by another organization if it is not satisfied with the results of that investigation

- Your organization may have the experience where information under your authority is affected by an unauthorized use of JUSTIN by someone else's employee. When this happens you will receive a report on the results of that organization's investigation. If you are not satisfied with the results of the investigation, you may request a review. Please refer to the *Unauthorized Use of Electronic Access* policy for the full text of the policies and procedures for requesting a review of an investigation into unauthorized use of electronic access to JUSTIN.

What could happen to an organization

Your organization could have its electronic access to JUSTIN suspended by the JUSTIN Access and Security Committee pending an investigation. If this happens, the JUSTIN Access and Security Committee will report its decision to suspend to your organization prior to the suspension being implemented.

Your organization could have its electronic access to JUSTIN immediately suspended, without notice, if the Information Technology Services Division, Ministry of Attorney General/Ministry of Public Safety and Solicitor General suspects an unauthorized use that may present an immediate and substantial risk of harm.

Investigation Report:

Unauthorized Electronic Access to JUSTIN

Date of Investigation Report:

Name of organization whose employee/contracted worker may have committed the unauthorized use:

Name of organization whose information may have been the subject of an unauthorized use:

Name of investigating Organization:

Contact person:
e-mail:
telephone number:

INCIDENT

1. **When did the suspected unauthorized access occur?**

2. **When and how was the suspected unauthorized use first identified?**

3. **What information was accessed?**

4. **What was the type of unauthorized use (i.e. creating, viewing, modifying, using, disclosing, or deleting)?**

5. **What were the consequences of the unauthorized use?**

6. **Were there any other significant results of the investigation?**

7. **Are there any recommendations or actions to be taken?**

8. **The names of other affected parties or bodies that will receive the report of the investigation**

#4 Revoking Electronic Access to JUSTIN

Electronic access to JUSTIN is carefully controlled, is subject to electronic access agreements, and is monitored. All organizations and JUSTIN users are made aware of the legal and policy requirements that govern JUSTIN when they are given electronic access. If an organization's actions or inactions, including unauthorized use of electronic access, result in a breach of an electronic access agreement it may be necessary to revoke electronic access to JUSTIN.

Responsibilities of an organization

An organization may revoke the electronic access of a JUSTIN user under their authority

- You may revoke the electronic access of an employee or contracted worker if that is the most appropriate action given the nature of their unauthorized use of electronic access. The *Revoking Electronic Access to JUSTIN* policy sets out the criteria that you will consider when making the decision whether or not to revoke the electronic access of your employee for unauthorized use of electronic access.

- You may revoke the electronic access of an employee or contracted worker because of a breach of the terms and conditions of your organization's electronic access agreement or other conduct. For example, if your employee was found to be a security risk to JUSTIN.

An organization may reinstate the electronic access of a JUSTIN user under their authority

- You may reinstate the electronic access of your employee. The JUSTIN Electronic Access Policy lists who you must report this decision to and what information must be included when reporting the decision.

An organization may recommend that a JUSTIN user employed by another organization have their electronic access to JUSTIN revoked

- Your organization may have the experience where information under your authority is affected by an unauthorized use of JUSTIN by someone else's employee. When this happens you will receive a report on the results of that organization's investigation. You may then recommend to that organization that they revoke the electronic access of their JUSTIN user. If the organization does not revoke the electronic access of their JUSTIN user, they are required to report their reasons to you in writing.

What could happen to an organization

If your organization's actions, or inactions, including unauthorized use of electronic access, result in a breach of an electronic access agreement it may be necessary to revoke your organization's electronic access to JUSTIN.

Contacts and Resources

The JUSTIN Access and Security Committee

The JUSTIN Access and Security Committee is responsible for managing electronic access to JUSTIN. If you have any questions about the JUSTIN Electronic Access Policy, you may send your question to the attention of the Chair of the JUSTIN Access and Security Committee at: AGCSBJACSCommittee@gems7.gov.bc.ca.